サイバーセキュリティの最先端の研究をしています

横浜国立大学大学院環境情報研究院/先端科学高等研究院
准教授 吉岡 克成

サイバーセキュリティシンポジウム2023

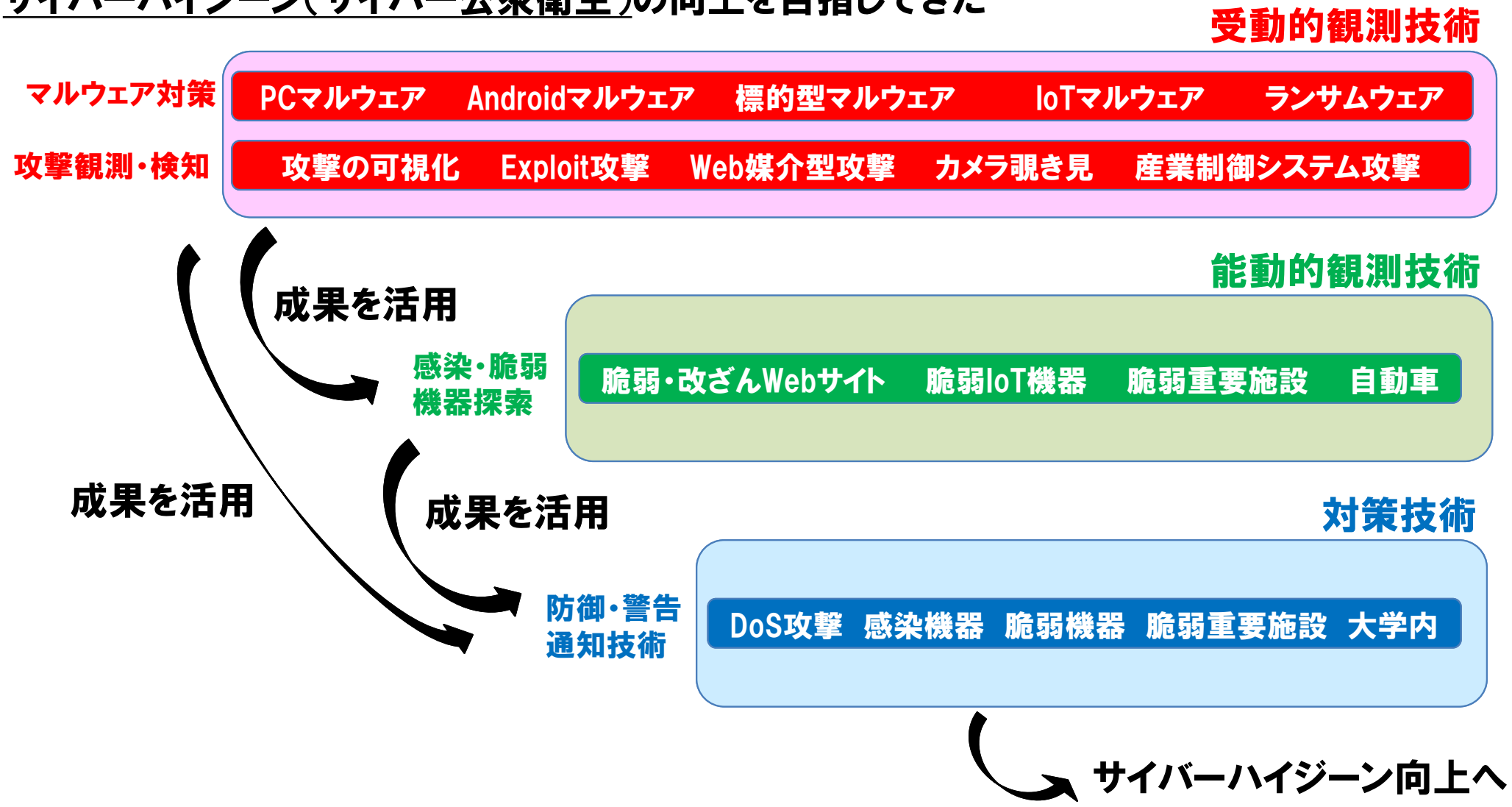
サイバーセキュリティ研究所
Cybersecurity Research Institute

横浜国大では…

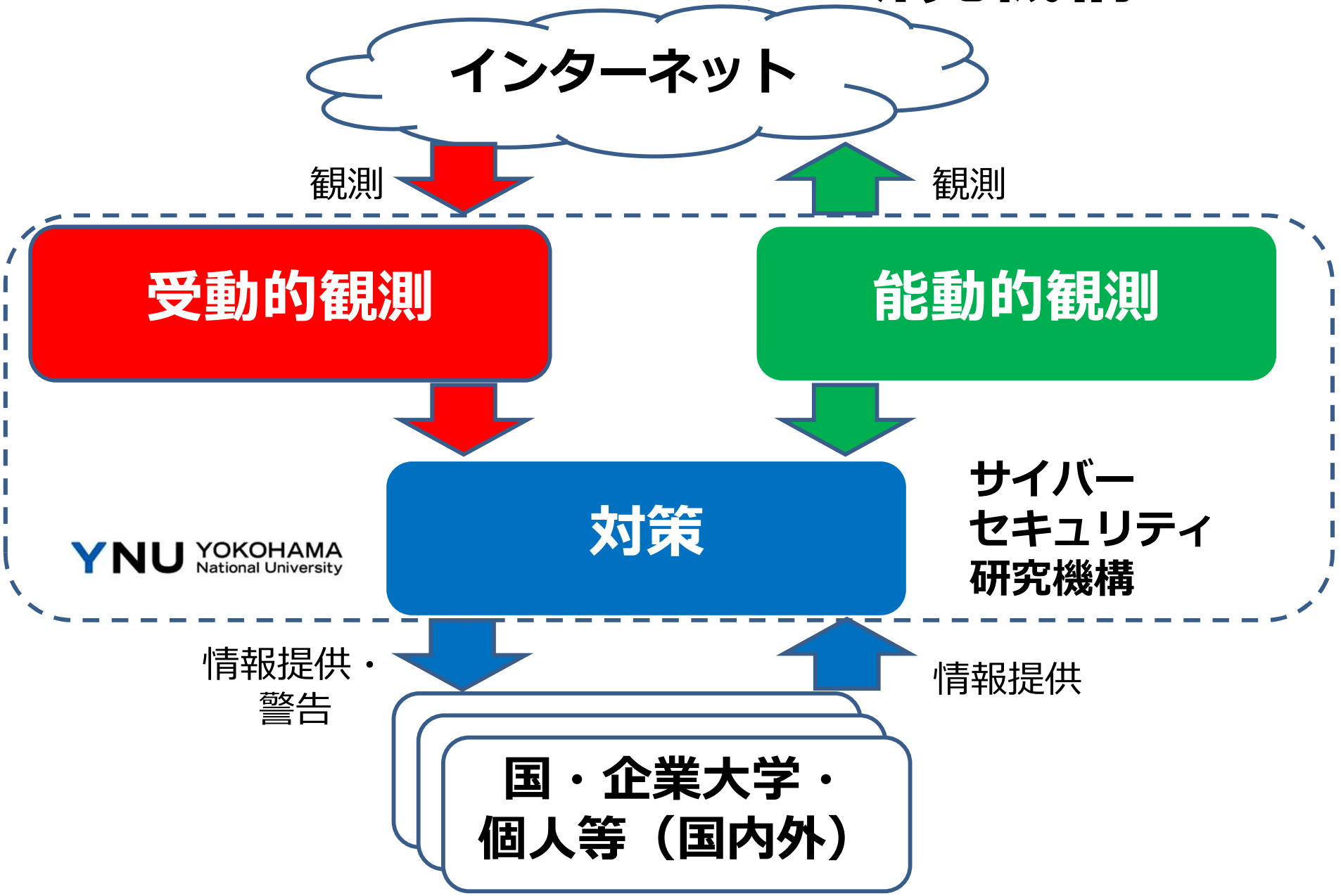
- 変遷を続けるサイバー攻撃やマルウェアの活動、脆弱な機器・システムを観測、分析、対策する仕組みを10年以上継続的に構築・運用してきました
- 本日は、これまでの活動で達成した事、足りない事、そして、今後目指したい事について、お話をさせて頂きたいと思います

これまでの研究活動: 概要

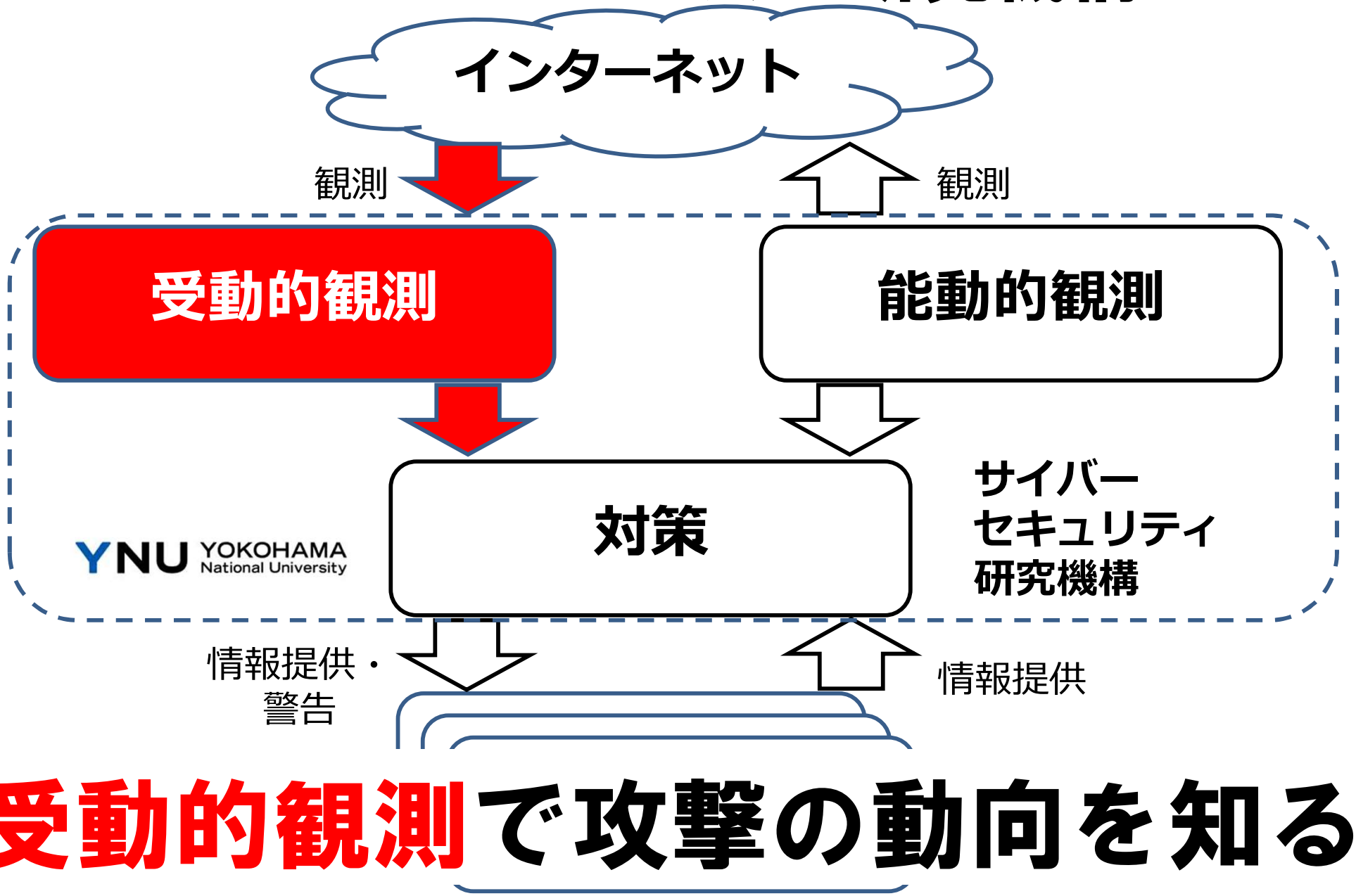
サイバー攻撃やマルウェアの観測のための「受動的観測技術」、感染した機器や脆弱機器を探索する「能動的観測技術」、関係者に状況を伝え防御を行う「対策技術」を軸に研究実施し、サイバーハイジーン(サイバー公衆衛生)の向上を目指してきた



横浜国大にて構築を進めてきた サイバーセキュリティ研究機構



横浜国大にて構築を進めてきた サイバーセキュリティ研究機構



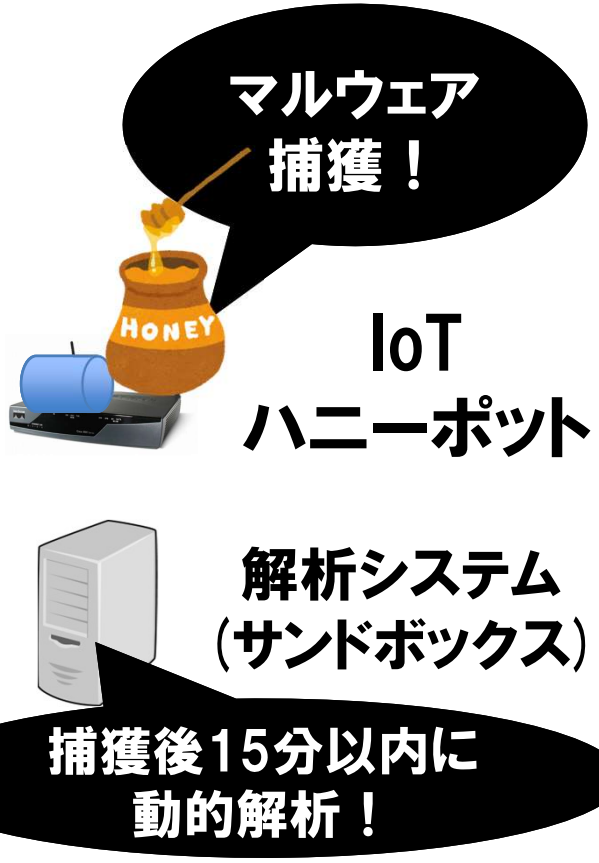
受動的観測で攻撃の動向を知る

IoTハニーポット (2015～)

IoT機器へのサイバー攻撃を観測する囮システム（IoTハニーポット）を世界に先駆けて構築・観測開始

攻撃元機器
（マルウェア
感染済）

攻撃者が用意
したサーバ



Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.
Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.

2016年のIoTサイバーパンデミックの予兆を1年前に把握

感染機器IPアドレス数/月

マルウェア Miraiの登場

1カ月133万 IPアドレス

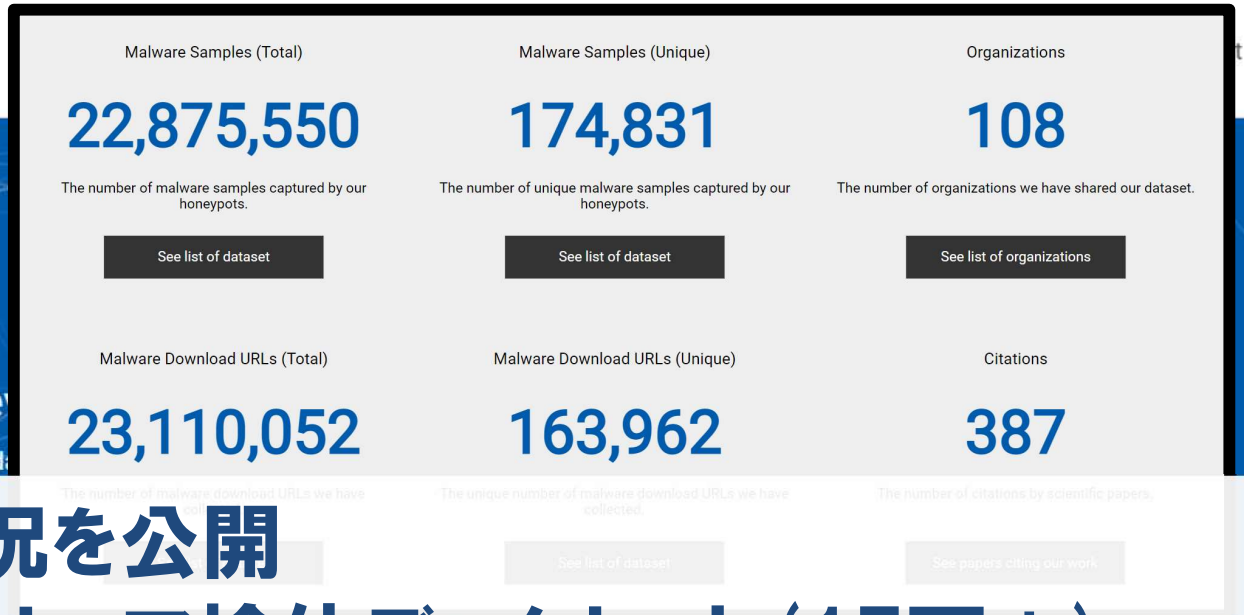
218か国・地域でIoT機器の感染を観測

IoTハニーポットに関わる数字

運用年数:	8年間
ハニーポット設置国・地域:	22か国・地域
累計収集検体数(ハッシュ値ベース):	274,822検体‡
マルウェアDL URL:	321,586 件‡
検体等提供組織数:	200 組織・個人
検体等提供先国数:	39か国・地域
学術論文引用件数†:	71.3件/年

‡ 2017/11～2022/9/18 現在での集計(EFLファイルのみ)
† 関連論文2件の平均参照件数(Google Scholarによる集計, 2022/9/18現在)

IoTマルウェア・攻撃情報提供サイト
https://sec.ynu.codes/iot



最新の観測結果の概況を公開
世界最大規模IoTマルウェア検体データセット（17万＋）、
マルウェアダウンロードURLを研究者・開発者向けに提供

re binaries)

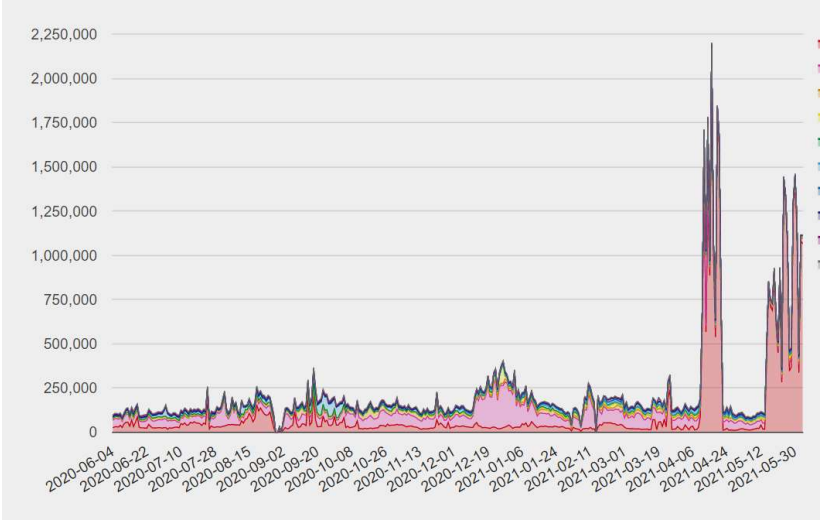
Dataset-2 (IoT honeypot: Malware download URLs)

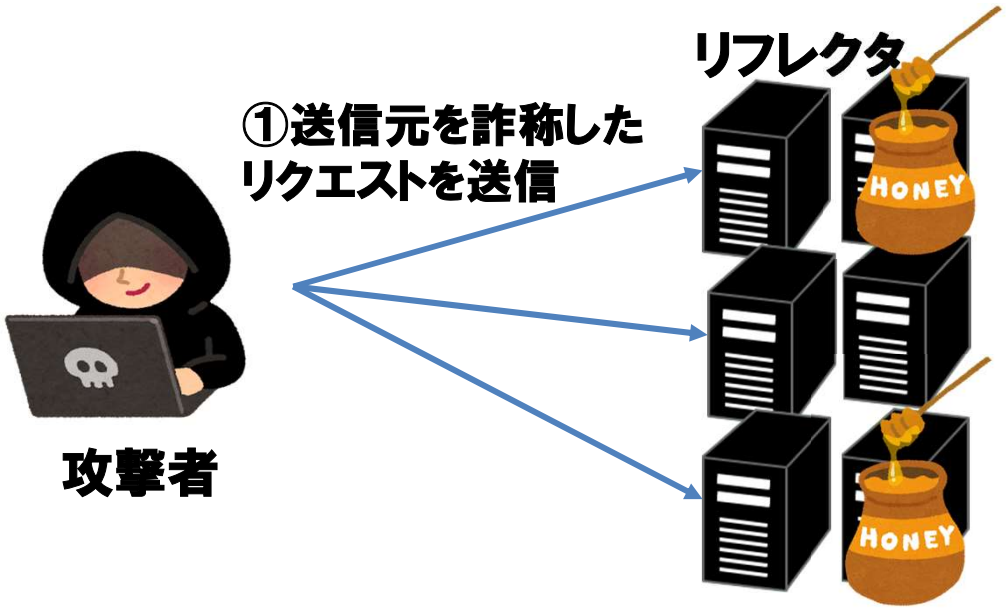
Amppot:サービス妨害攻撃観測用ハニーポット

踏み台に出来そうに見せかけたオープンサービスを用意して攻撃を観測する世界初の反射型サービス妨害攻撃観測機構を構築

約10万件/日、国内で約700件/日の攻撃を検知

攻撃検知時に世界130の公的対策機関、6000以上のネットワークオペレータに攻撃速報を発行





List of abused protocols observed by agnostic Amppot (Agnostic Amppot listens on all UDP ports and returns random strings)

Service	Port	#Attack
CLDAP	389	6656999
DTLS	443	53781
DNS	53	39168
WSD	3702	26775
ARMS	3283	24864
Dahua Discovery	37810	23868
MSSQL	1434	14816
STUN	3478	10346
Portmap	111	9785
NTP	123	7523

The table shows the number of attacks observed by agnostic Amppot over the last 7 days.

Lukas Kramer, Johannes Krupp, Daisuke Makita, Tomomi Nishizoe, Takashi Koide, Katsunari Yoshioka, Christian Rossow, "AmpPot: Monitoring and Defending Amplification DDoS Attacks," Proc. Research in Attacks, Intrusions, and Defenses (RAID15), Lecture Notes in Computer Science, Vol. 9404, pp. 615-636, 2015.

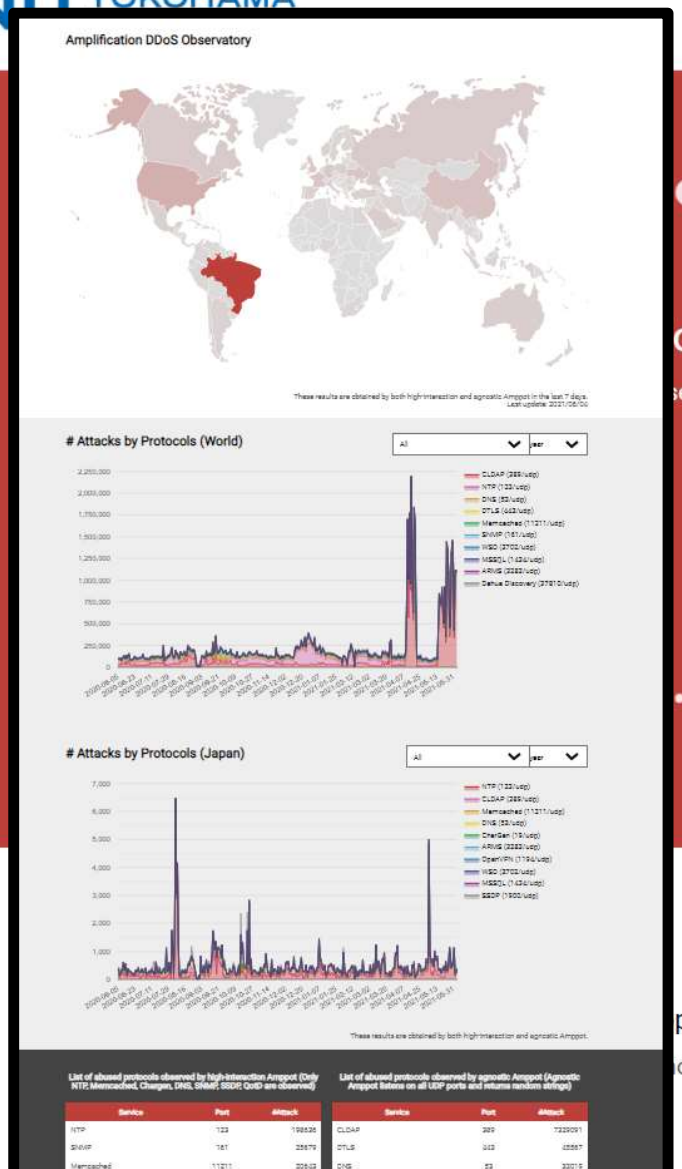
観測事例：国内への攻撃

- AnonymousによるOpKillingBay
  - 和歌山県太地町のイルカ漁への抗議活動.
- DD4BCによる企業の恐喝
  - DDoS攻撃を利用して企業を恐喝し，Bitcoinの身代金を要求.
- TOKYO2020
  - 2020年開催予定の東京オリンピックに関連するサイバー攻撃.
- ロシア系ハッカー集団KILLNET
  - e-Gov，地方自治体，IT/通信事業者への攻撃等

http://www.nikkei.com/article/DGXLASDG05H5W_V01C15A1CC1000/

https://www3.nhk.or.jp/news/html/20220907/k10013806691000.html

DoS攻撃情報提供サイト
https://sec.ynu.codes/dos



YNU YOKOHAMA

About News Datasets Contact

onitoring Amplification DDoS Attacks

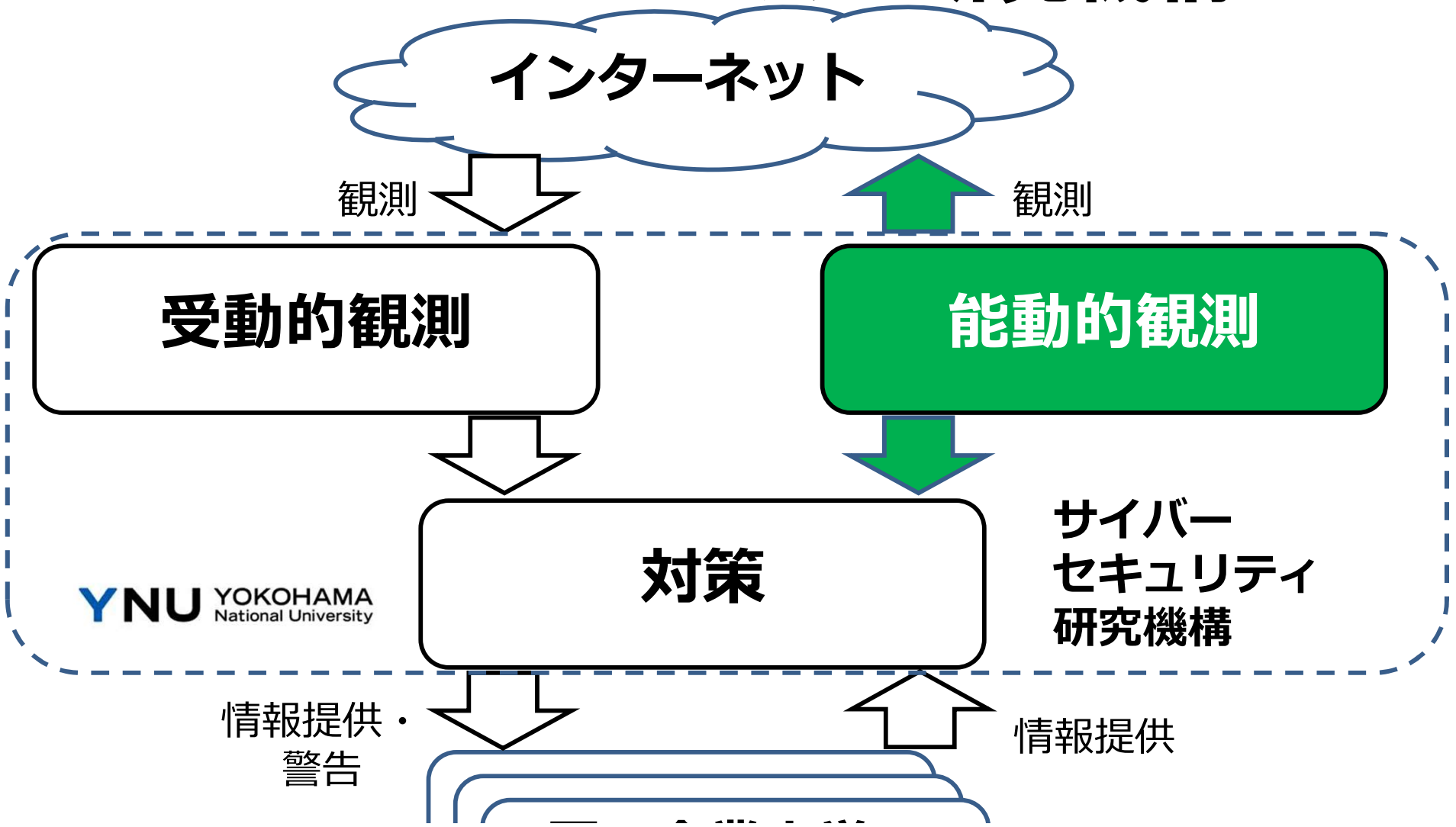
ervation results of Amppot, a honeypot for monitoring amplification DDoS Attacks [1].

最新の観測概況を公開
攻撃観測時にアラートを発出
（地震速報のサイバー攻撃版）
→ICT-ISAC、Shadowserver Foundation
を通じて世界130の公的対策機関、6000
以上のネットワークオペレータに提供中

SHADOWSERVER

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

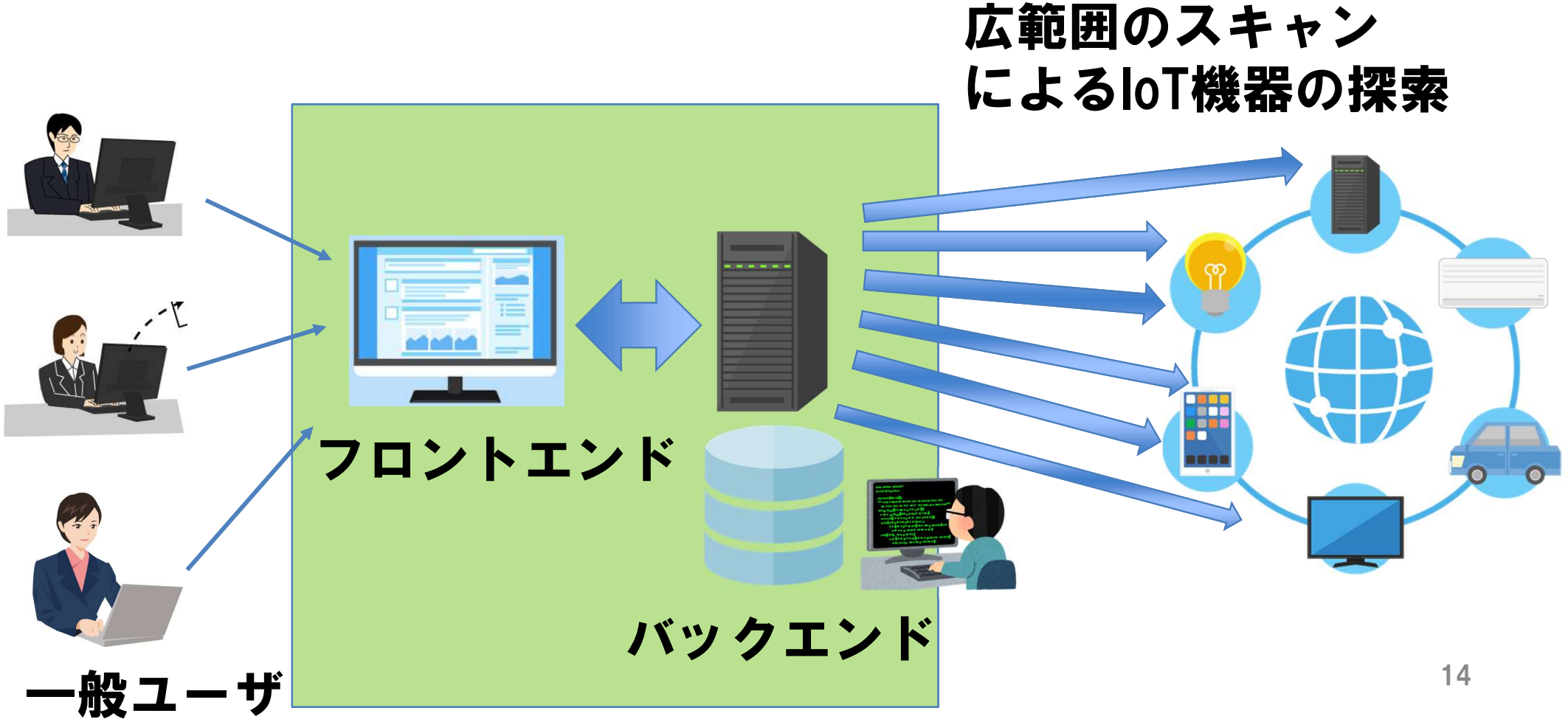
横浜国大にて構築を進めてきた サイバーセキュリティ研究機構



能動的観測で脆弱な機器を探索

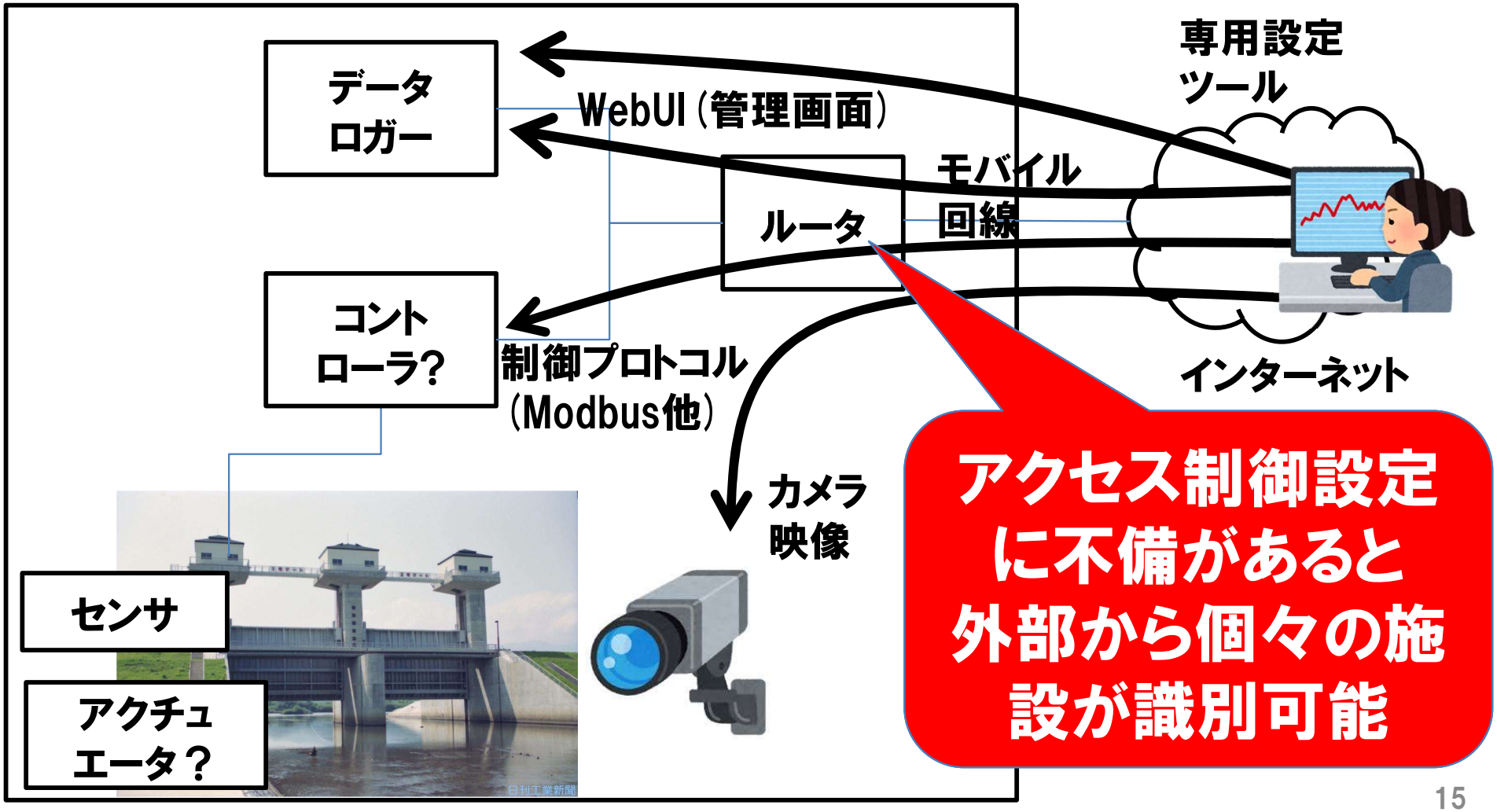
広域スキャンシステム

広域ネットワークをスキャンし、脆弱/設定不備のあるIoT機器等の探索を行うシステム



「重要IoT機器」とは？

治水、防災、発電など重要な施設の遠隔監視を行うためのデータロガーや制御機器



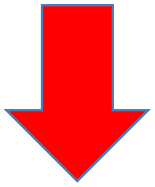
事例

水道 監視システム


事例:
流入河川ゲート

2017年度　総務省重要IoT機器調査

（重要機器候補）150件



2020年度総務省重要IoT機調査

（重要機器候補）924件

これらの機器は、世界的に著名な既存の広域スキャンシステム（米国Shodan/Censys等）では検知できない

一般社団法人ICT-ISAC,脆弱な状態にある重要IoT機器の調査及び注意喚起について(報告)
https://www.ict-isac.jp/news/news20210901.html

海外の重要IoT機器の探索

米国のモバイルISPをシードに全世界探索を実施した結果、わずか１ラウンドの探索で**8機種3875件**を発見

Device model	Manufacturer	# Devices
[redacted] System Controller	[redacted] Systems	5
[redacted] System	[redacted] Systems	3
[redacted] Solar [redacted]	[redacted] Systems	39
Power[redacted]	[redacted] electric	1,019
[redacted] Receiver	[redacted]	1,204
[redacted] Tower Lighting System	[redacted] TECHNOLOGY	34
Aqui[redacted]	[redacted] LLC	1,531
Unknown model	Unknown manufacturer	40

半数以上は米国内の機器であり、一部に空港などの重要施設への設置を示唆する記載があったため、注意喚起の第一弾として**US-CERTに情報提供**を実施．数日のうちにIPアドレス所有者への注意喚起が完了した旨の返信があった

車載器の探索結果

- 2ラウンドの探索で12機種2,532件を発見
- いずれも車載ルータ/GW

Manufacturer	Device name	Build-in/Retrofit	#devices	Top countries/regions	Top ASes
1	A	Retrofit	278	NL 26.0% SE 18.9% US 16.3%	CELLCO-PART / KPN KPN National
2	B	Retrofit	391	ES 59.0% MA 20.3% DE 11.9%	VODAPONE_ES / DTAG internet service
3	C	Unknown	821	US 96.5% BR 2.2%	CELLCO-PART
3	D	Unknown	85	US 84.3%	CELLCO-PART / CELLCO
4	E	Unknown	186	IT 59.1% DE4.0%	VODAPONE-IT-ASN
4	F	Unknown	88	DE	
5	G	Retrofit	104	US ES AU	N-
6	H	Built-in	5	TW 1	
7	I	Retrofit	360	ES 9	N-
8	J	Unknown	3	DE 1(	et
5	K	Retrofit	67	US 51.5% FR 19.6% CN 9.0%	CELLCO / CELLCO-PART
9	L	Built-in	144	ES 99.9%	VODAPONE_ES / TELEFONICA_DE_ESPANA

主に欧米のモバイル回線で発見

Takahiro Ueda, Takayuki Sasaki, Katsunari Yoshioka, and Tsutomu Matsumoto, "An Internet-wide View of Connected Cars: Discovery of Exposed Automotive Devices," Proc. The 2nd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I 2022), 2022.

発見された車載ルータ/GWのセキュリティ

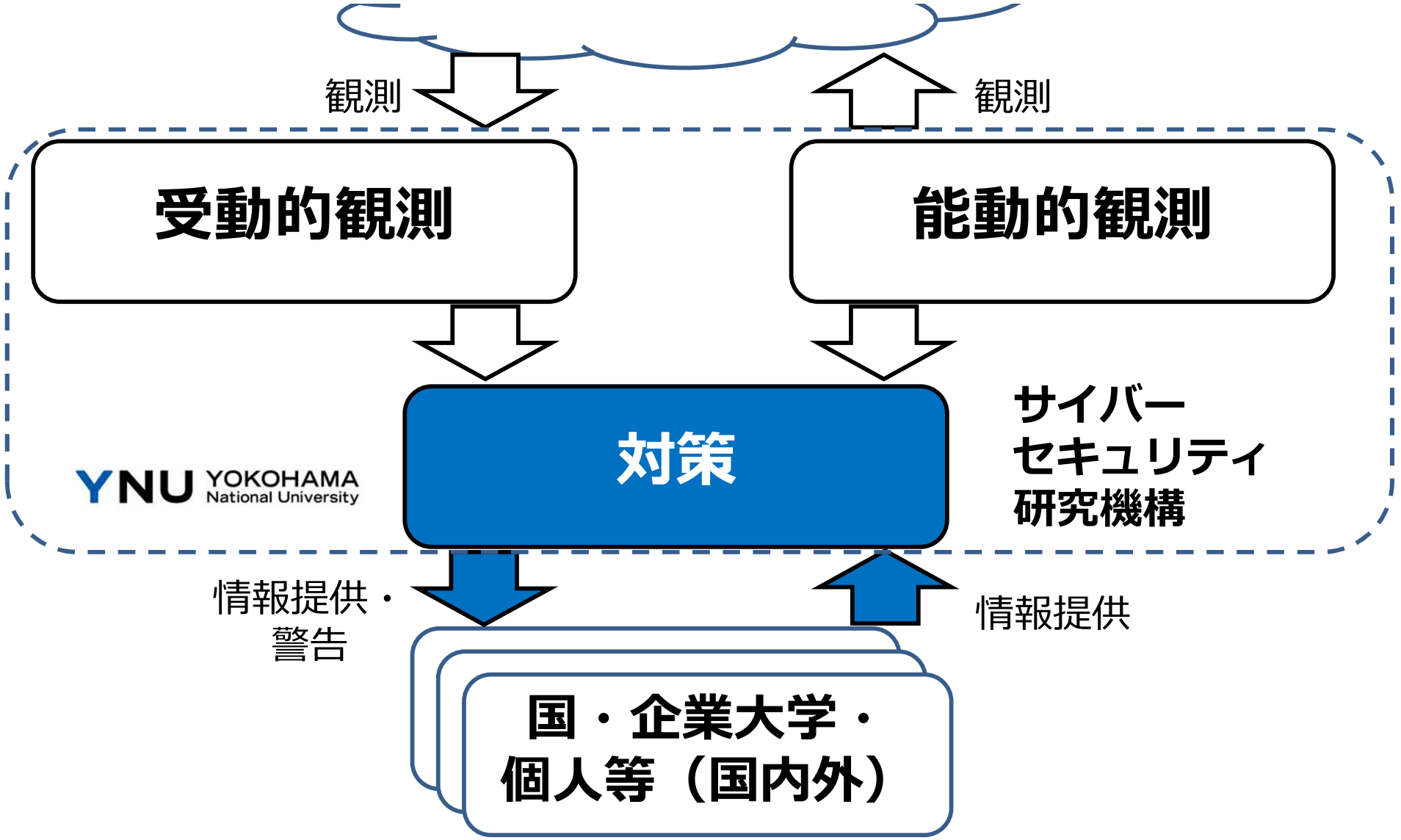
- 5機種でTelnetが動作し、外部からアクセス可能
- 8機種で古い組み込みWebサーバプログラム稼働（管理画面露出）
- 9機種では車内の車載NWに接続可能（2機種は接続確認）
- 3機種でGPS情報が閲覧可能（自動車の位置が把握可能）

Table 5: The risk of the discovered OBE products

Device name	Outdated protocol	Outdated software	Weak default password	Connection to in-vehicle networks	Information exposure
A	-	Tlideslash monit 5.0	-	confirmed	Running process
B	Telnet	OpenSSH 5.1	-	confirmed	Location, ignition, etc
C	-	Anonymized server name 1	✓	-	-
D	-	Anonymized server name 2	✓	-	-
E	FTP, Telnet	PHP 5.6.31 light httpd 1.4.39	-	possible	-
F	Telnet	PHP 5.6.31 light httpd 1.4.39	-	possible	-
G	Telnet	-	-	possible	Location
H	-	-	-	possible	-
I	-	PHP 5.3.10	-	possible	-
J	FTP	CrushFTP	-	-	-
K	Telnet	-	-	possible	Location
L	FTP	-	-	possible	-

Takahiro Ueda, Takayuki Sasaki, Katsunari Yoshioka, and Tsutomu Matsumoto, "An Internet-wide View of Connected Cars: Discovery of Exposed Automotive Devices," Proc. The 2nd International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I 2022), 2022.

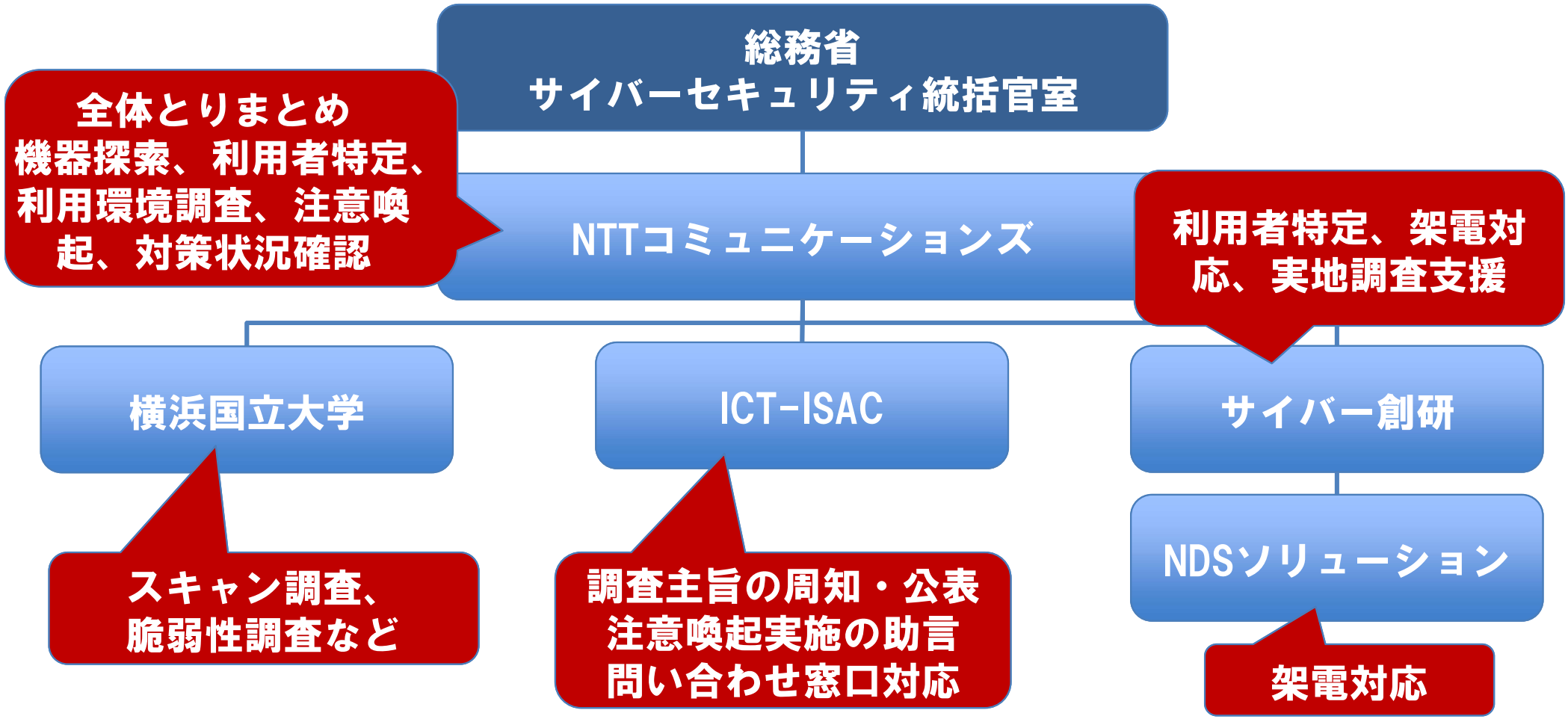
対策でサイバーハイジーン（公衆衛生）を向上させる



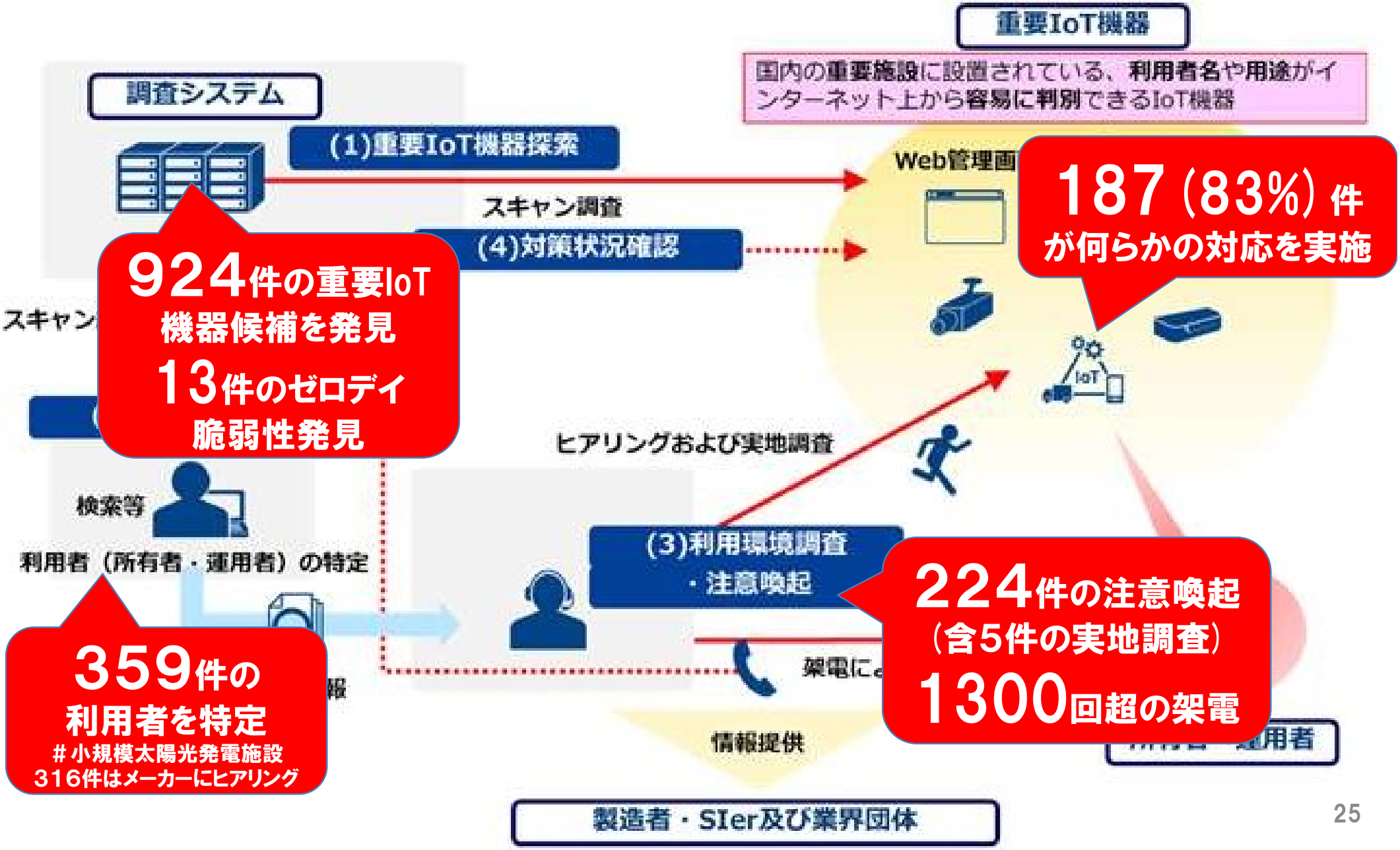
総務省重要IOT機器調査および注意喚起2020

ICT-ISAC, 脆弱な状態にある重要IoT機器の調査及び注意喚起について
https://www.ict-isac.jp/news/news20200728.html
ICT-ISAC, 脆弱な状態にある重要IoT機器の調査及び注意喚起について(報告)
https://ict-isac.jp/news/news20210901.html

体制


総務省
サイバーセキュリティ統括官室
全体とりまとめ
機器探索、利用者特定、
利用環境調査、注意喚
起、対策状況確認
NTTコミュニケーションズ
利用者特定、架電対
応、実地調査支援
横浜国立大学
ICT-ISAC
サイバー創研
NDSソリューション
スキャン調査、
脆弱性調査など
調査主旨の周知・公表
注意喚起実施の助言
問い合わせ窓口対応
架電対応

脆弱な状態にある重要IoT機器の調査及び注意喚起(2020)



利用者の意識と注意喚起活動

Q.部外者に閲覧・操作されることを意識しているか？

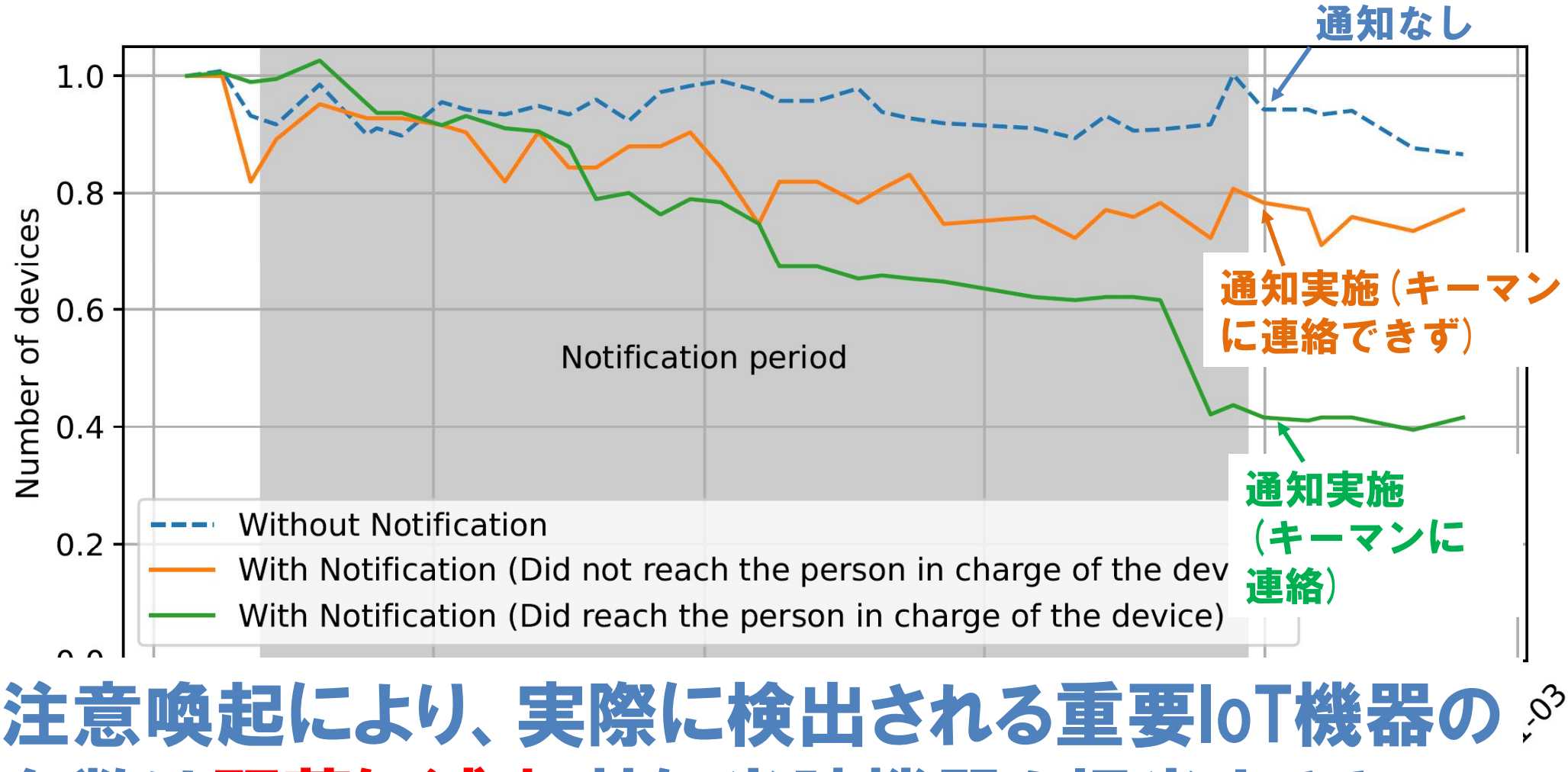
【A】部外者に閲覧・操作されることを意図しているか				181	
	意図している			18	10%
		対策するか	はい	4	22%
			いいえ	13	72%
	意図していない			163	90%
		対策するか	はい	139	85%
			いいえ	22	13%

9割の利用者は、重要IoT機器が部外者に閲覧されることを意図していない

→しかし、指摘すれば85%は対応する意思を示す

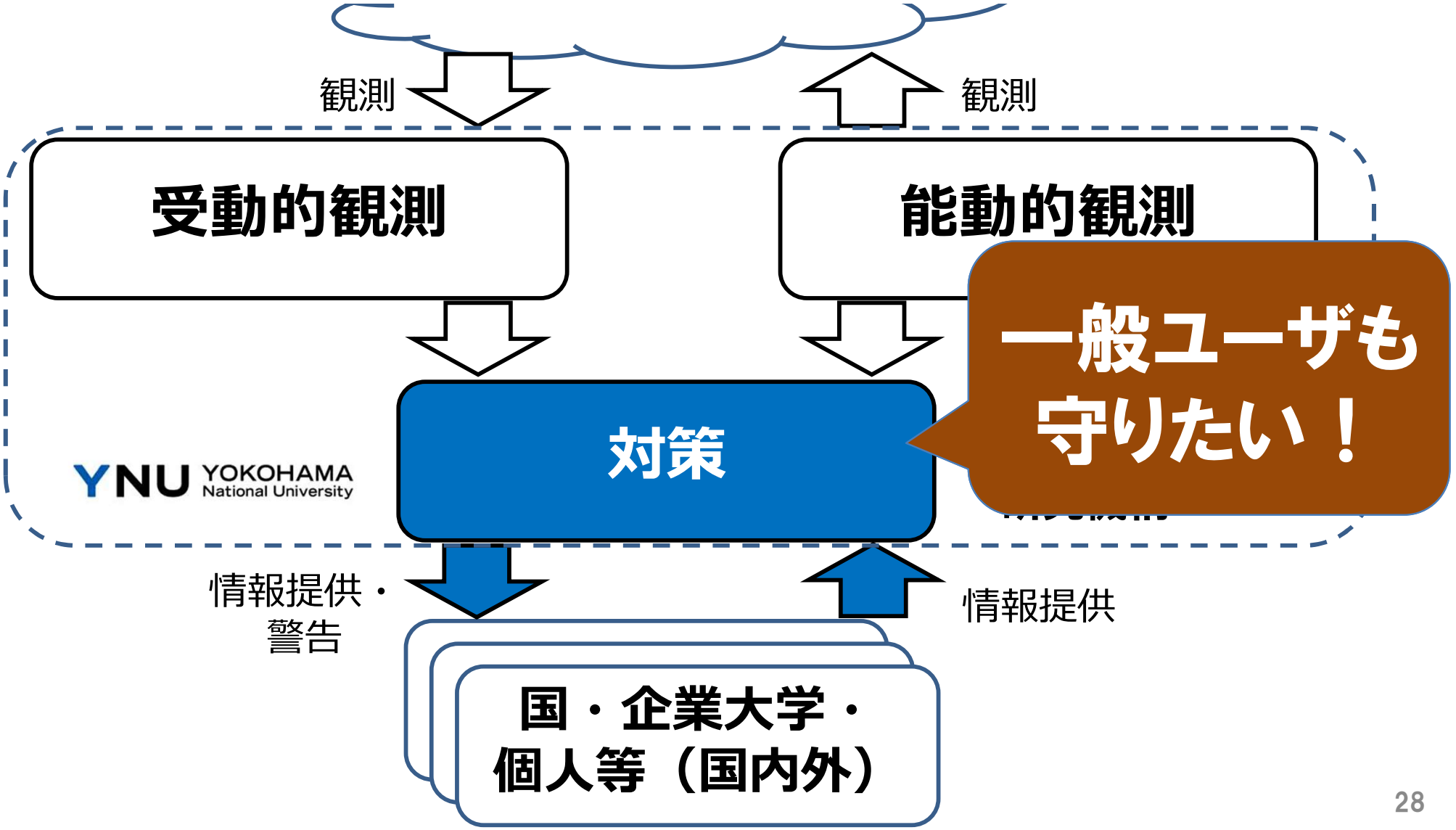
→注意喚起活動の意義が大きいと言える

重要IoT機器の検出台数



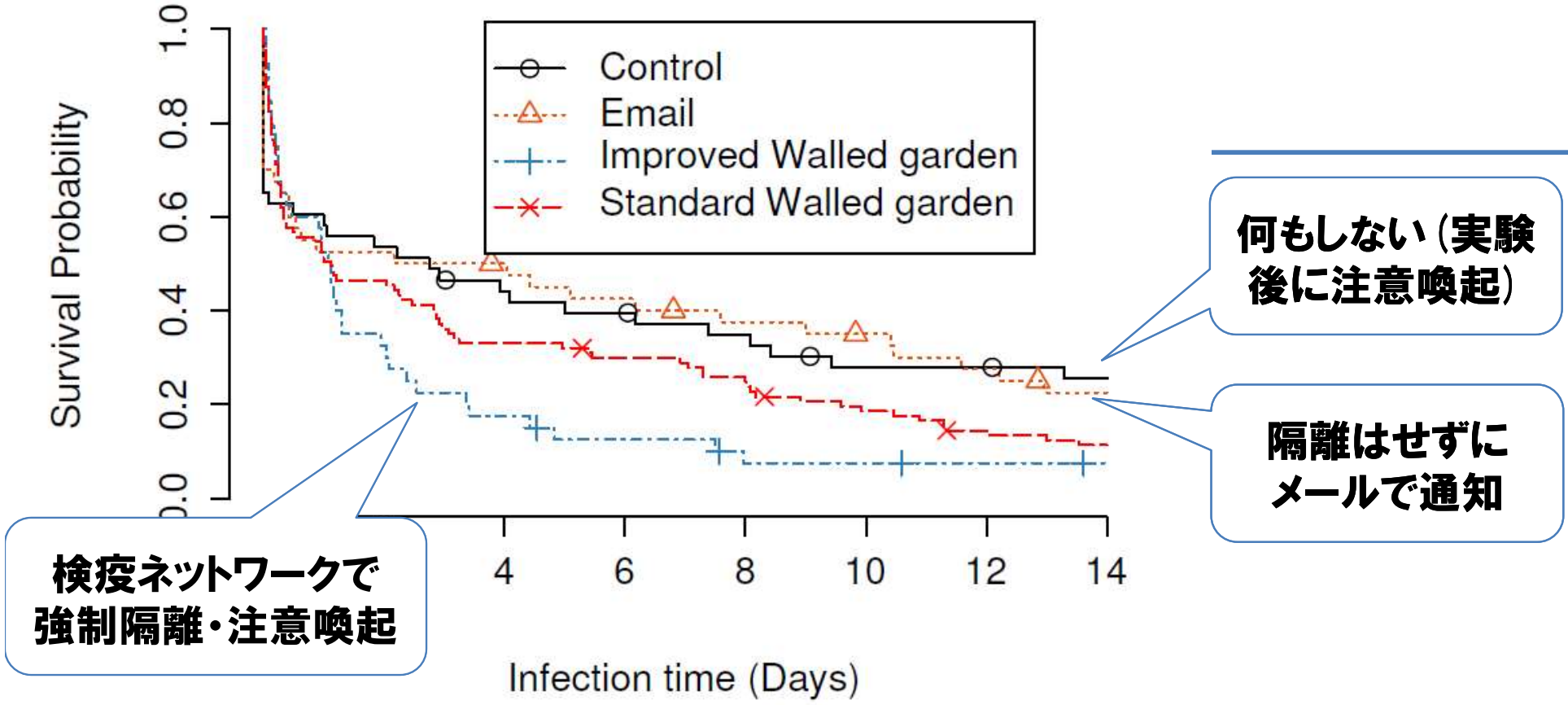
注意喚起により、実際に検出される重要IoT機器の台数は**顕著に減少**.特に当該機器を担当するキーマンに連絡できた場合は効果が高い

対策でサイバーハイジーン（公衆衛生）を向上させる



オランダISPとの連携と Walled Garden（検疫NW）の活用

O. Cetin, C. Gañán, L. Altena, D. Inoue, T. Kasama, K. Tamiya, Y. Tie, K. Yoshioka, M. van Eeten, "Cleaning Up the Internet of Evil Things: Real-World Evidence on ISP and Consumer Efforts to Remove Mirai," The Network and Distributed System Security Symposium (NDSS 2019), 2019 (Distinguished Paper Award).



何もしない（実験後に注意喚起）

隔離はせずにメールで通知

検疫ネットワークで強制隔離・注意喚起

検疫NW強制隔離による注意喚起で高い感染抑制効果が確認

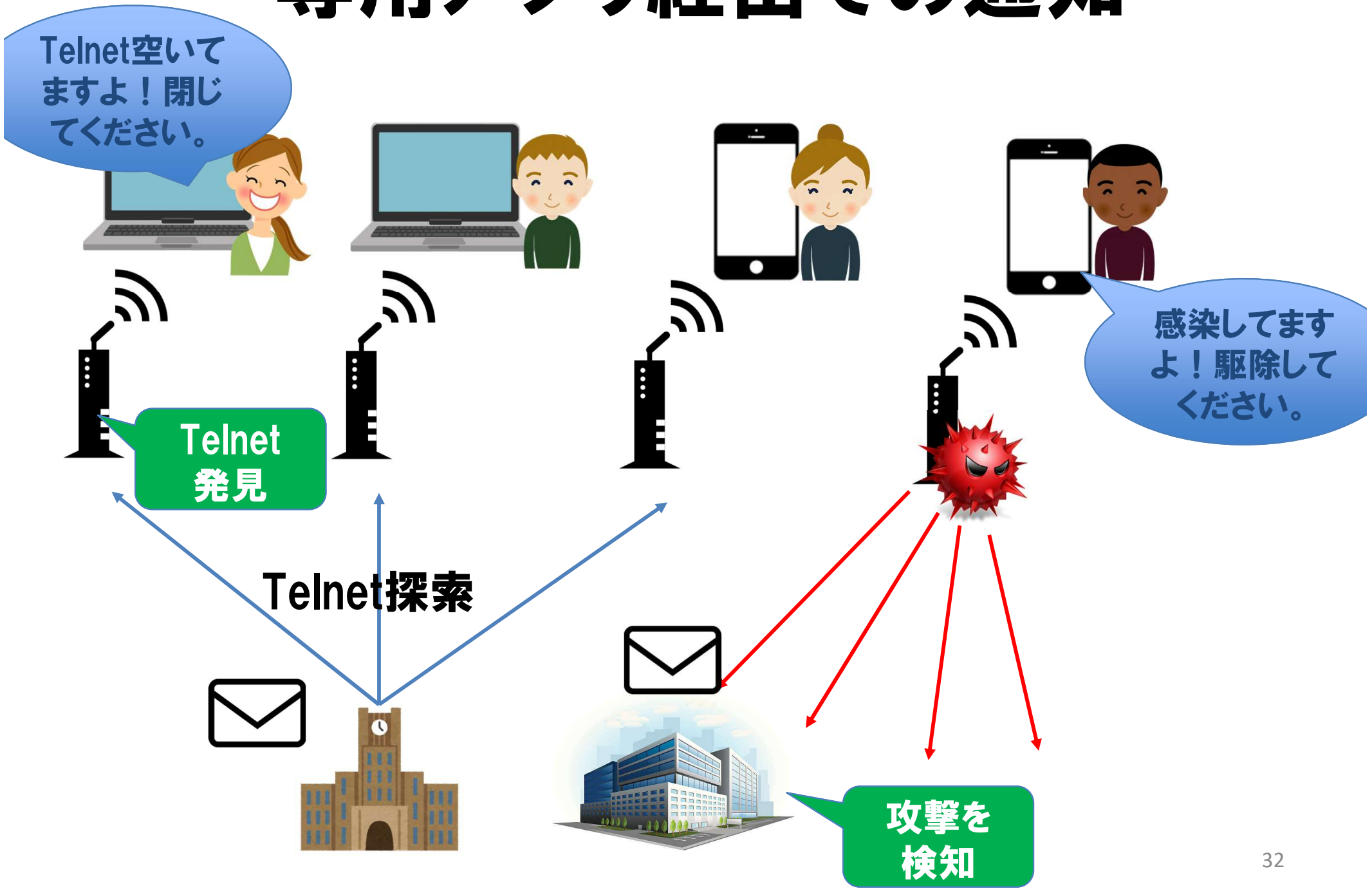
Figure 5: Number of infected devices on the ISP's consumer market before and after the notification experiment

NICT　WarpDriveプロジェクト

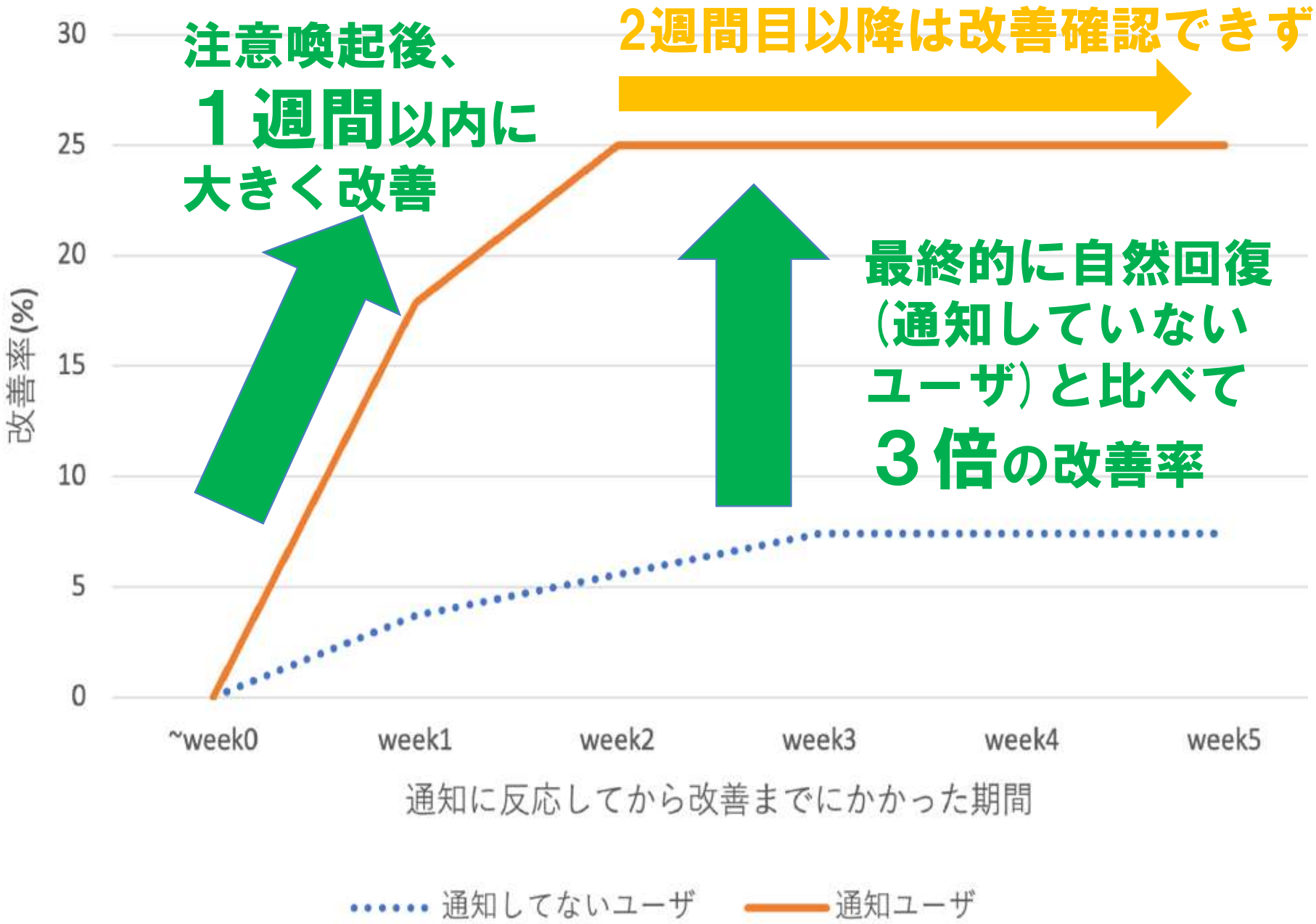
H28-R2に実施されたNICT委託研究プロジェクト.
R4からはNICTによるWarpDrive 2.0が開始.
タチコマ セキュリティエージェント(SA)をインストールして
誰でも実証実験に参加可能

https://warpdrive-project.jp/

専用アプリ経由での通知



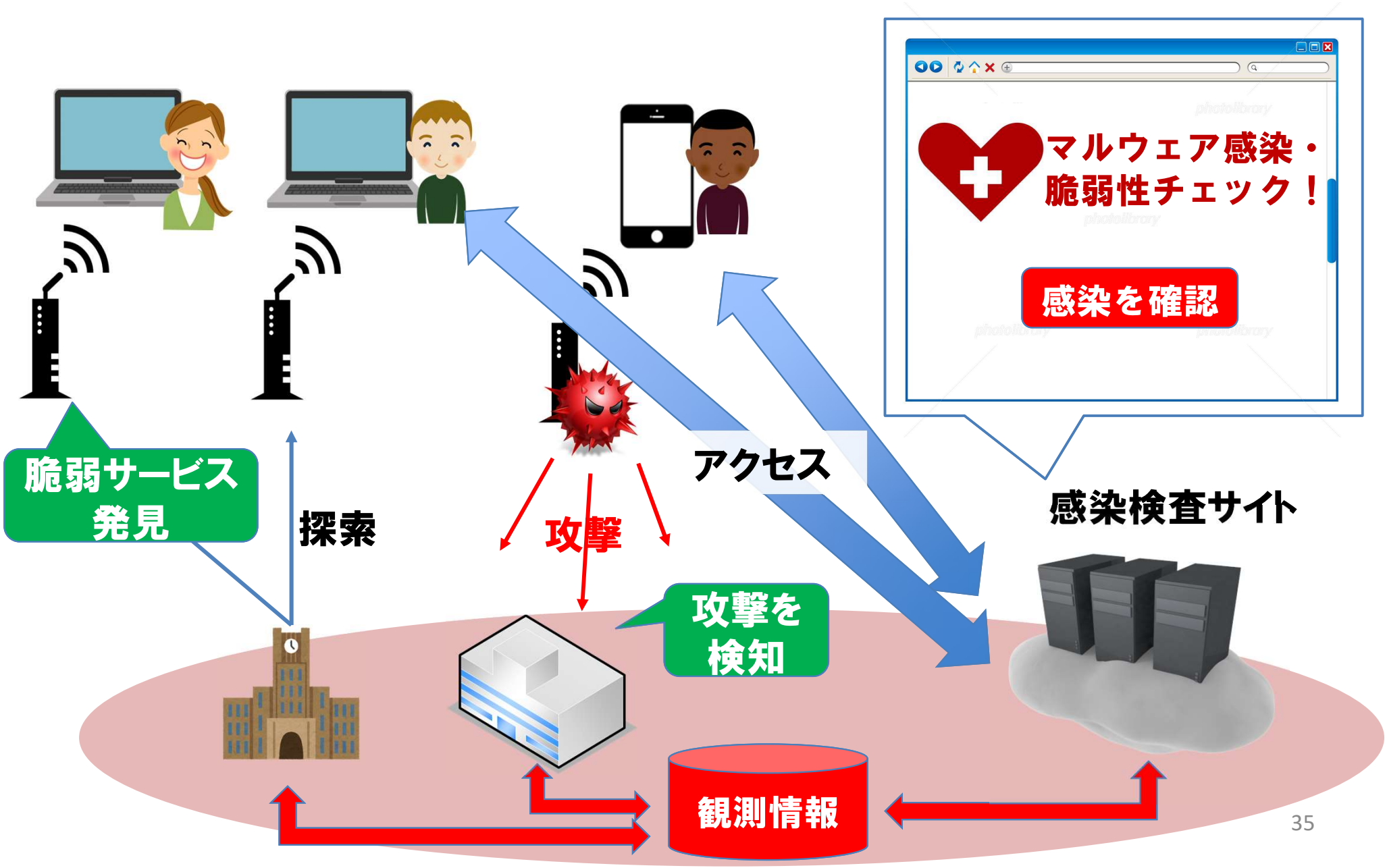
注意喚起による改善効果



専用アプリの事前インストールが必要であるため、普及に時間が掛かる

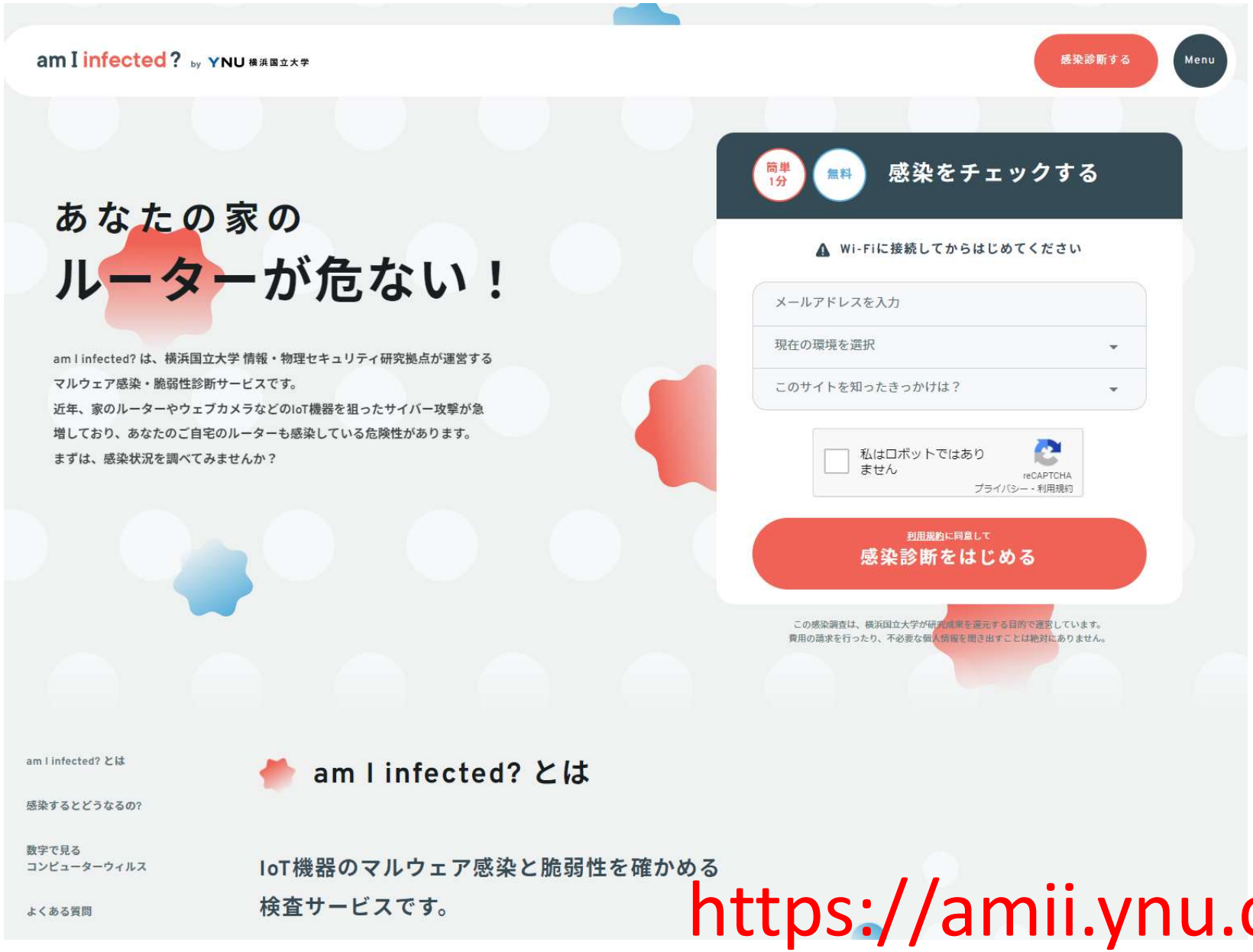
アプリなしで注意喚起・情報提供できないか？

感染検査Webサービス



NICT CYNEX (Co-Nexus A)の枠組みでご提供頂いたNICTERダークネットデータを活用

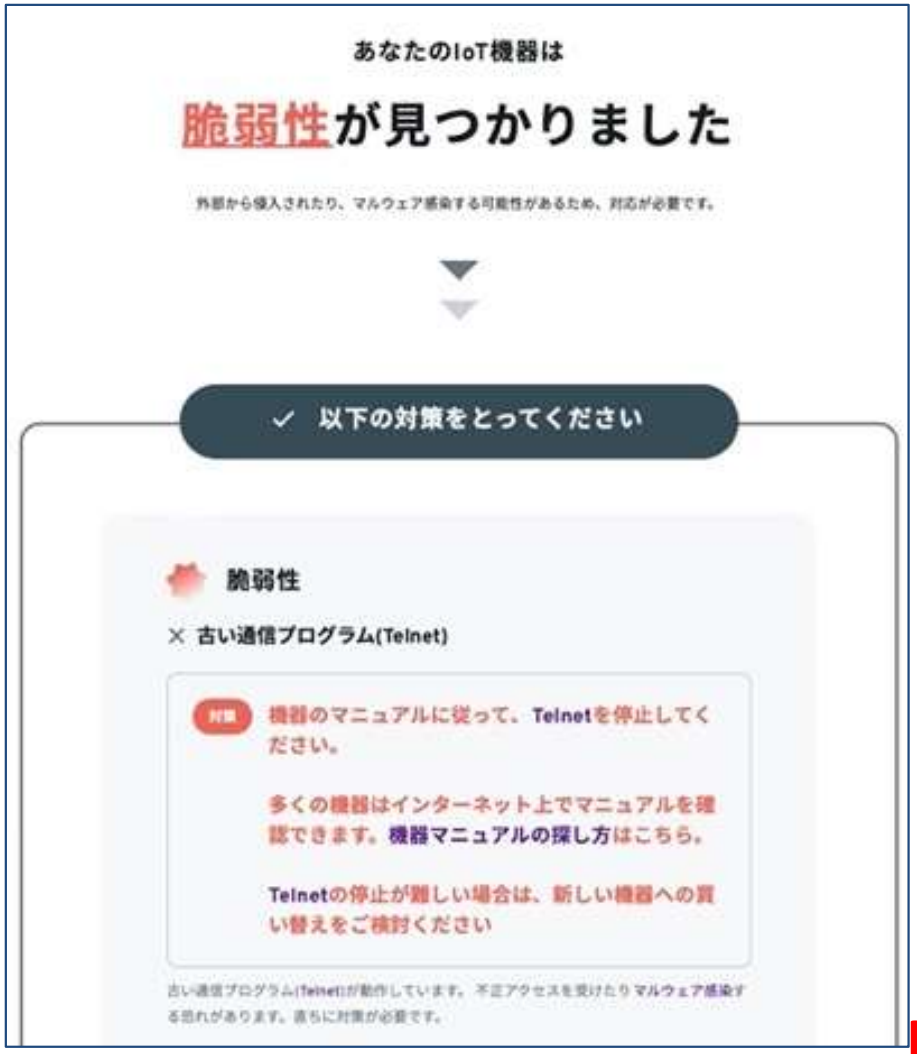
感染・脆弱性検査サービス
“am I infected?”

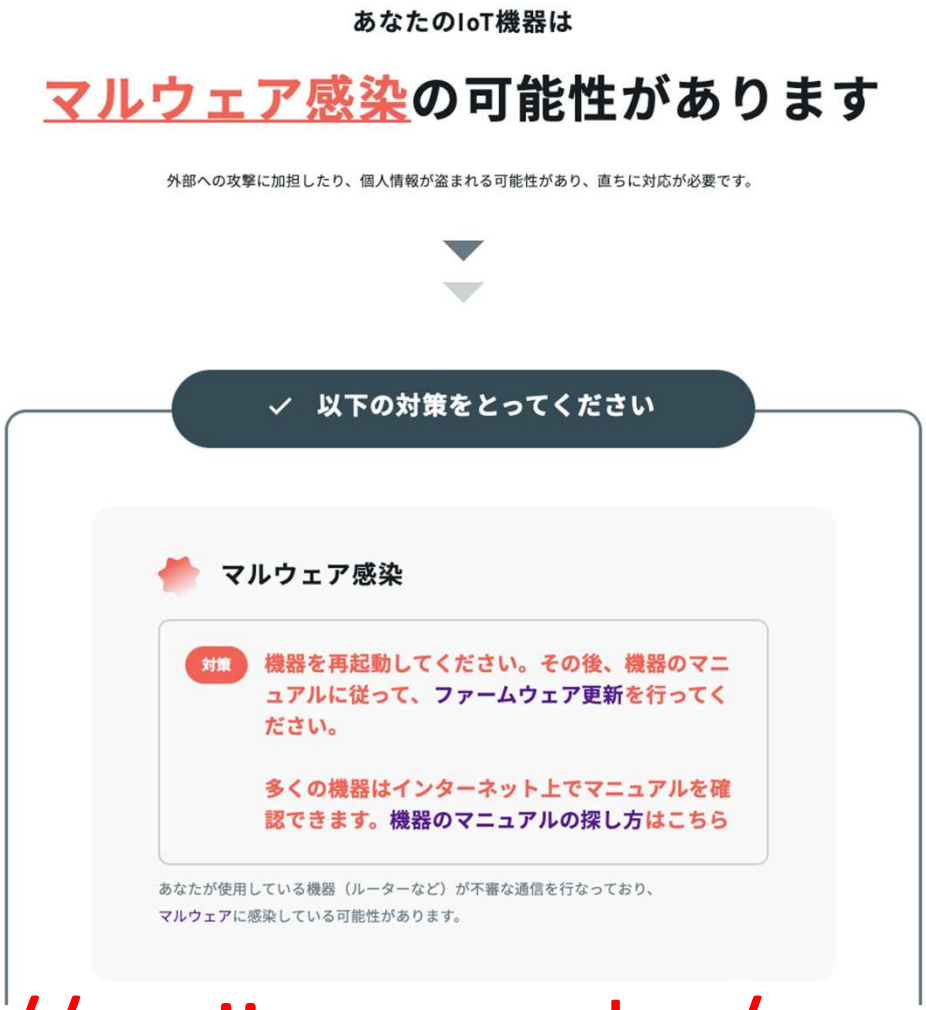


https://amii.ynu.codes/

問題が見つかった場合

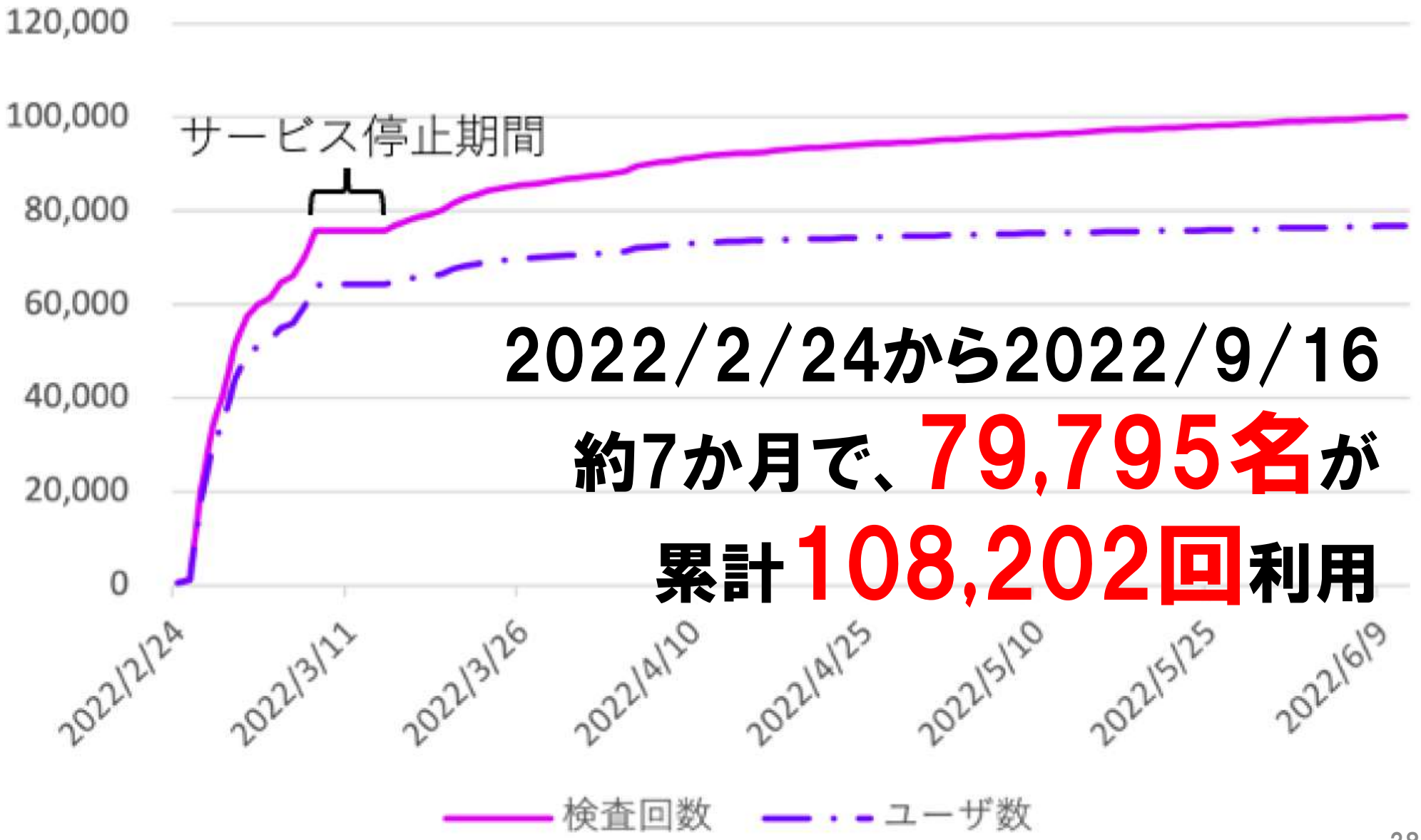
マルウェア感染また脆弱性発見の問題がある場合、問題点の説明と推奨する対策を提示する





https://amii.ynu.codes/

2022年2月サービス開始以降の利用状況



2022/2/24から2022/9/16

約7か月で、79,795名が

累計108,202回利用

感染機器、脆弱機器　検知状況

感染検知数：

89 人（0.12%）

脆弱性検知数：

293 人（0.38%）

脆弱性の種類	ユーザ数
古い通信プログラム（Telnet）*	73
メーカサポート終了*	63
管理者のパスワードが未設定*	2
既知の脆弱性*	24
古いファームウェア	91
初期 ID が公知	112
初期の認証情報が公知	79
初期の Wi-Fi パスワードが脆弱	29
認証が必要ない機器	1

＜脆弱性を有していた機器種別＞
ルーター：5社28種類
ウェブカメラ： 2社12種類
NAS：3社45種類
ファイアウォール：1社1種類

注意喚起効果

注意喚起効果が確認できるのは、再検査を行ったユーザのみ。
＃感染検査については最初の検査から24h後以降でないと効果を確認できない

感染検知数：　感染検知数（再検査有）

89 人 → 26 人（29.2%, 24h～）

脆弱性検知数：　脆弱性検知数（再検査有）

293 人 → 95 人（32.4%）

ユーザ全体の再検査率は18.4％であるため、セキュリティ問題が発見されたユーザは再検査率がそれぞれ3.4倍（感染）、1.8倍（脆弱性）と総じて高くなっている

注意喚起効果

注意喚起効果が確認できるのは、再検査を行ったユーザのみ。

＃感染検査については最初の検査から24h後以降

24h以降に再検査有

感染検知数 → **再検査時に感染無**

26 人 → **24 人（92.3%改善）**

再検査有

脆弱性検知数 → **再検査時に脆弱性無**

95 人 → **51 人（53.7%改善）**

稲澤朋也，佐々木貴之，吉岡克成，松本勉，"am I infected? エンドユーザに注意喚起を促すIoTセキュリティ診断Webサービスの実証実験，情報処理学会コンピュータセキュリティシンポジウム2022，2022.

これまでの研究活動のまとめ

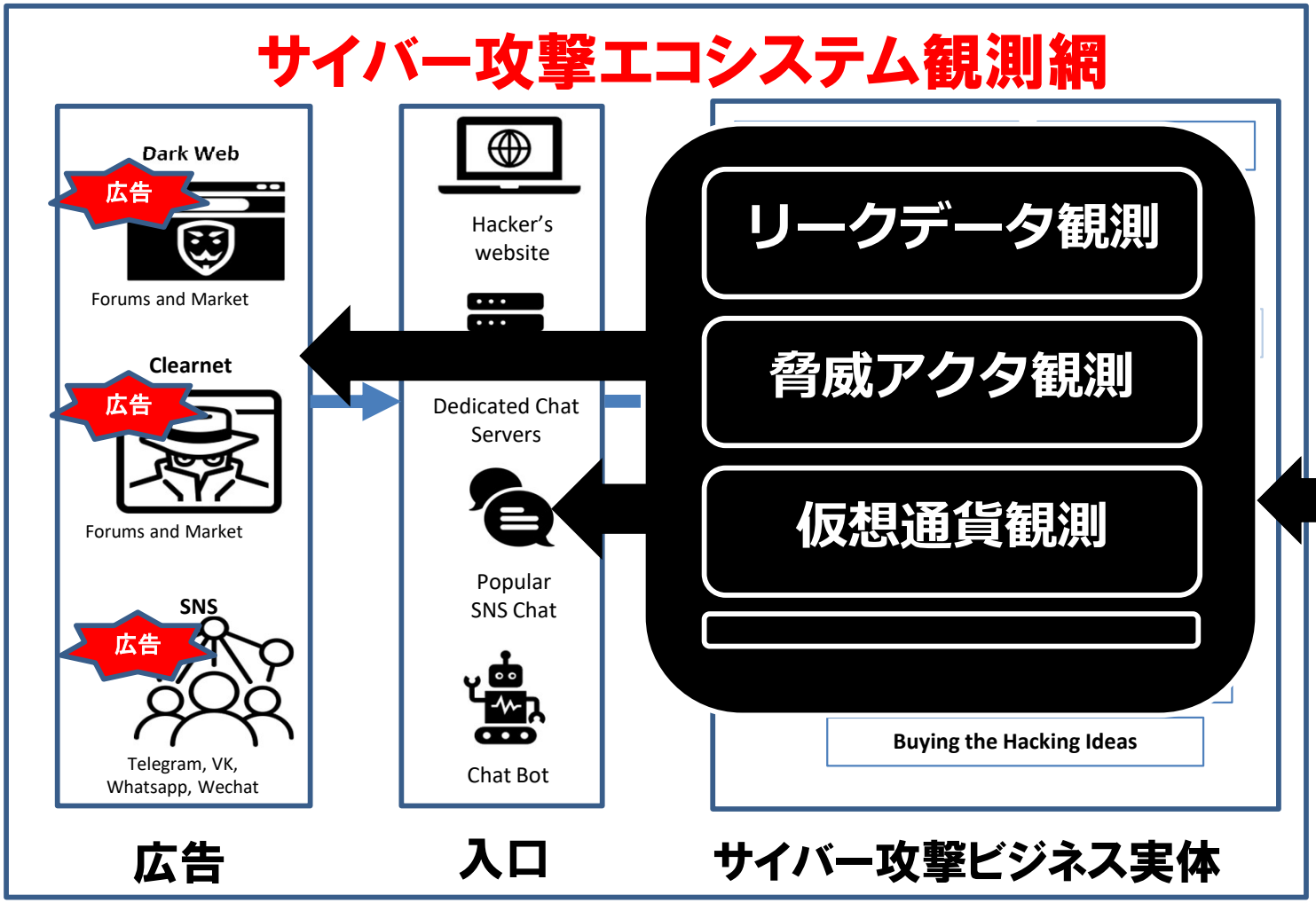
- **受動的観測**、**能動的観測**にサイバー攻撃を実際に調査し、その実態を明らかにすると共に、詳細分析に基づき、その実態を明らかにすることを主な研究アプローチとしてきた
- 現在は特に、観測、分析結果をいかに社会的に還元し、実際のセキュリティ向上に役立てるかの**対策**に焦点をあて、IoTのサイバーセキュリティのベースラインを高める「サイバーハイジーン（サイバー公衆衛生）」の概念に着目し研究を実施

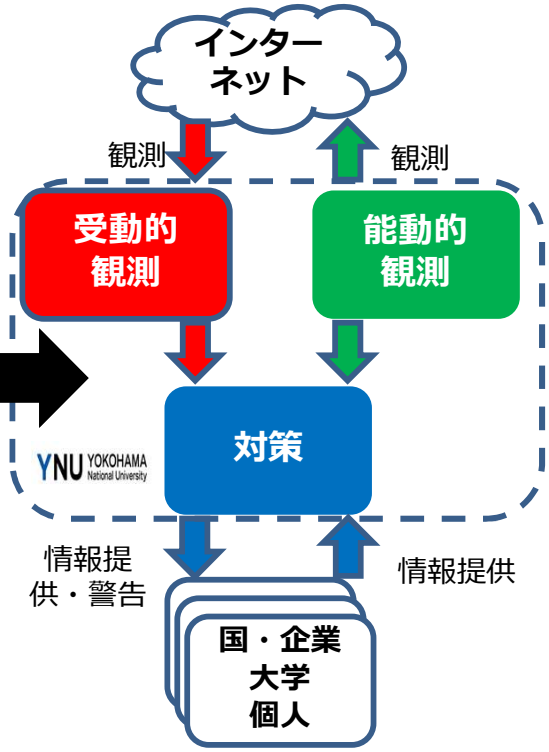
- **これからは？**

サイバー攻撃
エコシステム観測網

横浜国大にて構築中の サイバー攻撃エコシステム観測網

サイバー攻撃の原因となっているエコシステムを把握し、全体像を捉える





リークデータ観測事例

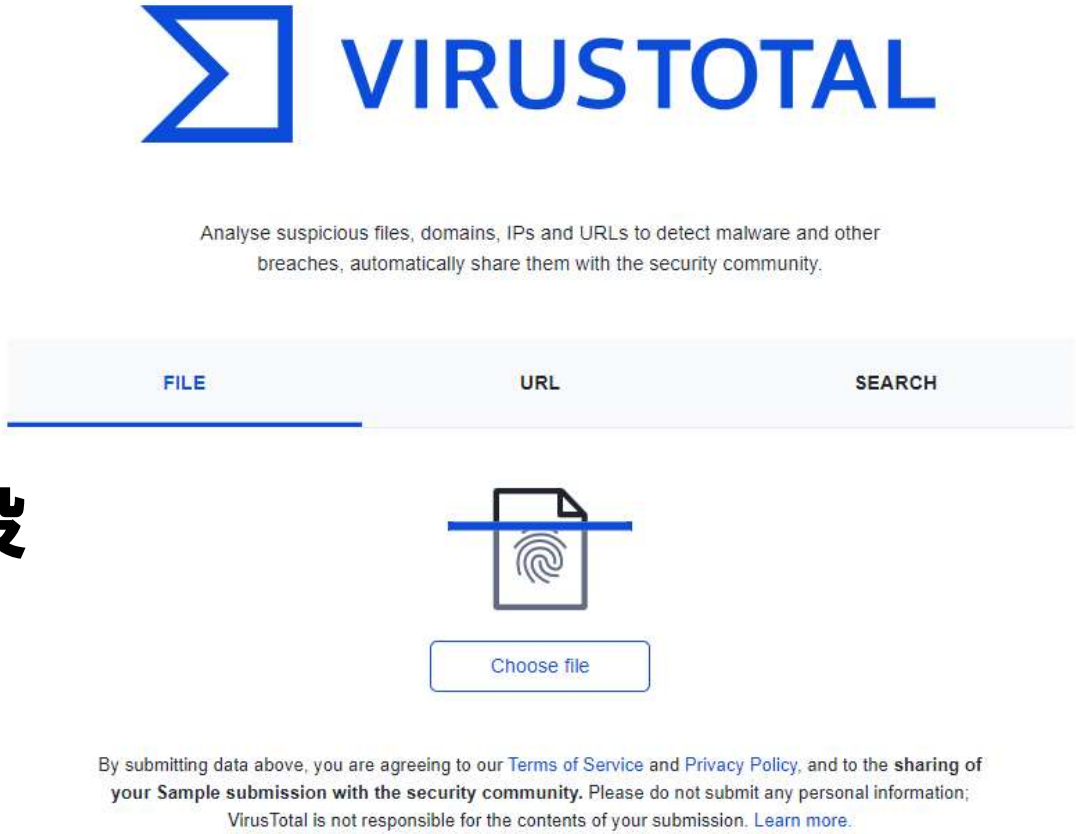
脅威アクタ観測
～IoTサイバー攻撃ビジネスの例～

ハニーポット検体解析結果と脅威アクタ観測の連携事例

サイバーインテリジェンスが集まる
エコシステムを作る

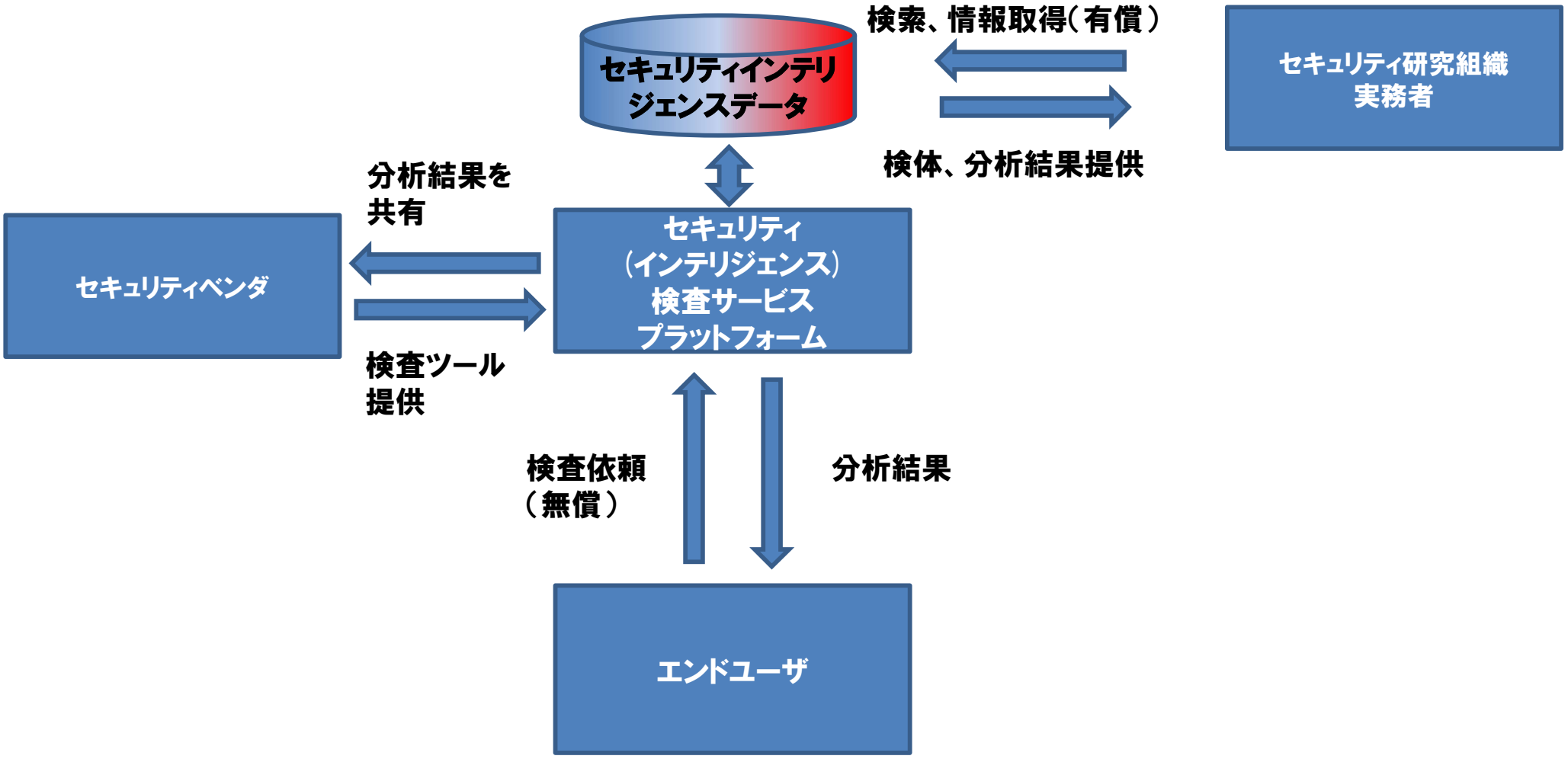
サイバーセキュリティデータ収集が研究開発を促進している好例

- Google社 Virus Total（ウイルストータル）



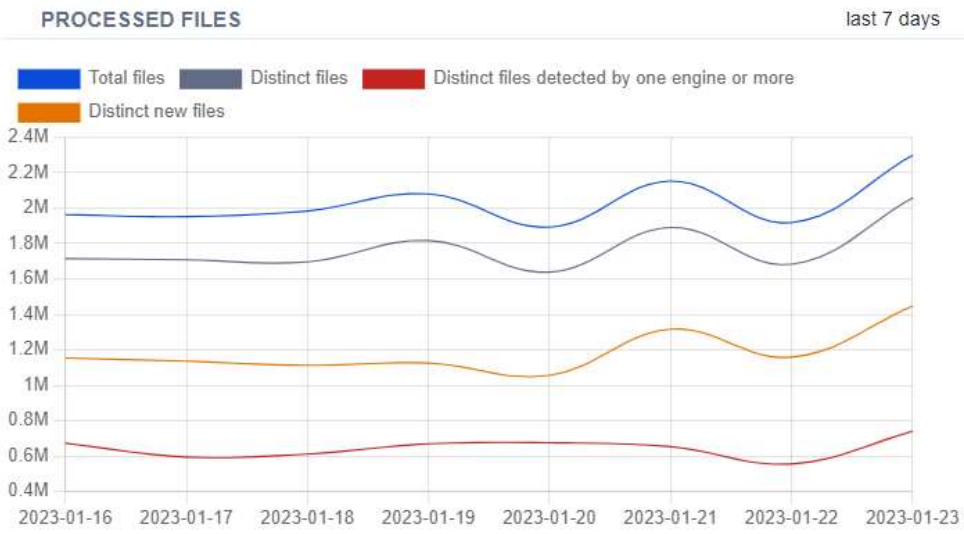
- 怪しいファイルやURLを投稿すると**70を超える**セキュリティソリューションで検査をして、結果を教えてくれる（利用は無料）

ウイルストータル全体像

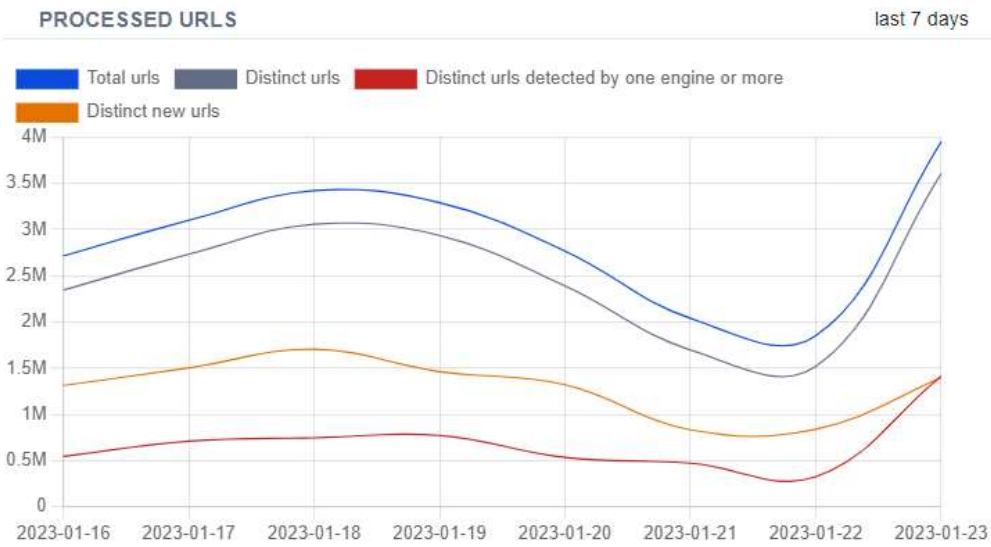


エンドユーザのサービス利用状況（無償）

ファイル検査依頼



URL検査依頼



VirusTotalには一日200万件以上の投稿（検査依頼）がある

提案：
日本版VirusTotalを
作れないか？

本家VirusTotalとの違いは？

1.日本への脅威に特化

2.様々な情報の検査・検証

3.コントロールドシェア

1.日本への脅威に特化

- 日本の企業、大学が分析エンジン、インテリジェンスを提供する

- 標的型メール、国内IoT機器への攻撃、フィッシング攻撃、SNS詐欺など国内で特徴のある脅威について、検査対象に対する有益な情報を提供することで海外の検査サービスと差別化を図る

2. 様々な情報の検査・検証

- ニュースや情報の信ぴょう性の検査
- 画像、動画、音声の真正性評価（ディープフェイク検知）
- ChatGPT or not?
- 偽ショッピングサイト、オンライン詐欺、不正に悪用されている電話番号
- なりすましメール、フィッシング検知

原理的には、専門家による判断が必要なすべての検査が対象となり得る。様々な分野の研究者を巻き込むことで多様な分析エンジンを用意する。研究者から見ると、サービスに投稿されたリアルなデータを使って研究を行うことができる。

3. コントロールドシェア

日本の企業等にこのサービスを利用してもらうためには、ウイルストータルのように投稿したデータが自由に共有されるのでは安心してサービスが使えない
→コントロールドシェアモードを提供

平成 28 年 6 月 22 日

重要インフラ事業者等 御中

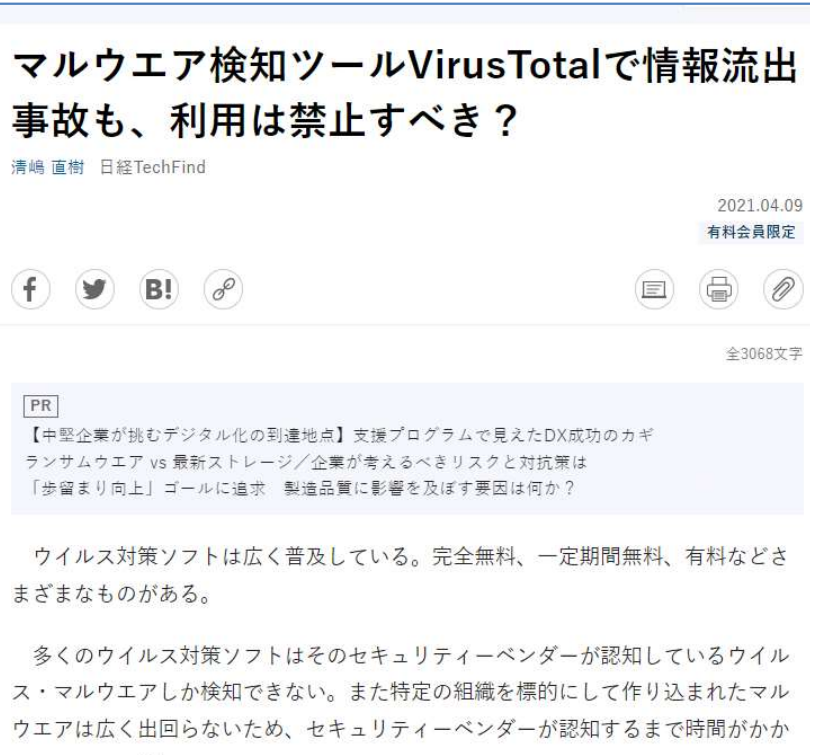
内閣官房サイバーセキュリティセンター
重要インフラグループ

VirusTotalへの機微情報アップロードに関する注意喚起

VirusTotal(※1)にアップロードされたファイルは、マルウェア判定の結果にかかわらず、契約をしたユーザー(※2)であれば、誰でもダウンロードできる状態となります。

このため機微情報を含むファイル等を不用意にVirusTotalにアップロードしないようご注意ください。また誤ってアップロードしてしまった場合は、速やかにVirusTotalに削除申請するなどの対応をお願いいたします。

※1 ファイルをアップロードするとマルウェアに感染していないか無料でチェックできる Web サービス。(https://www.virustotal.com/ja/)



マルウエア検知ツールVirusTotalで情報流出事故も、利用は禁止すべき？

清嶋 直樹　日経TechFind

2021.04.09
有料会員限定

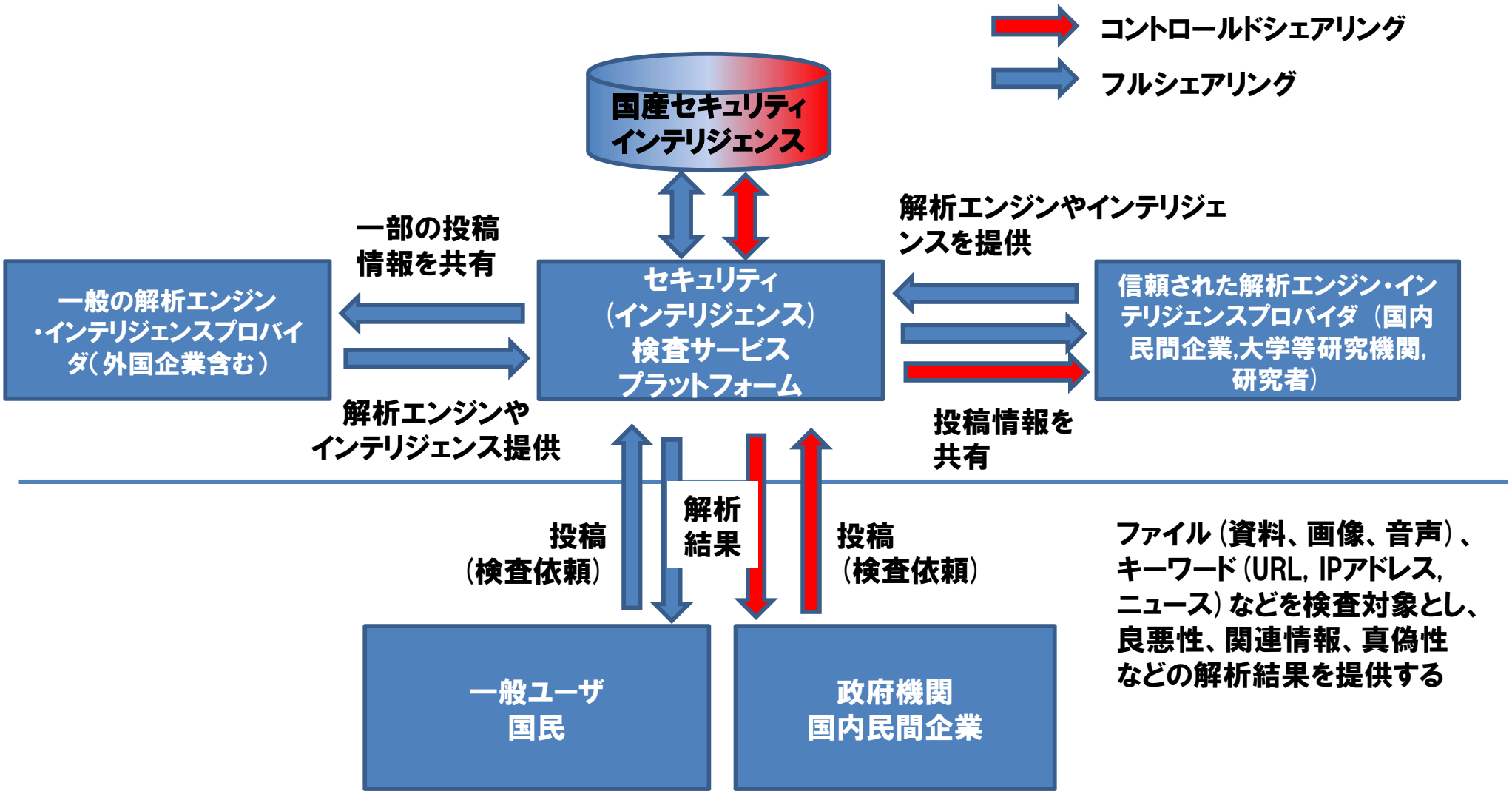
全3068文字

PR
【中堅企業が挑むデジタル化の到達地点】支援プログラムで見えたDX成功のカギ
ランサムウエア vs 最新ストレージ／企業が考えるべきリスクと対抗策は
「歩留まり向上」ゴールに追求　製造品質に影響を及ぼす要因は何か？

ウイルス対策ソフトは広く普及している。完全無料、一定期間無料、有料などさまざまなものがある。

多くのウイルス対策ソフトはそのセキュリティーベンダーが認知しているウイルス・マルウエアしか検知できない。また特定の組織を標的にして作り込まれたマルウエアは広く出回らないため、セキュリティーベンダーが認知するまで時間がかか

全体像



ファイル（資料、画像、音声）、キーワード（URL, IPアドレス, ニュース）などを検査対象とし、良悪性、関連情報、真偽性などの解析結果を提供する

期待される効果

- 投稿された情報を蓄積することで**国産のセキュリティインテリジェンスを構築**し、経済安全保障に寄与することができる。

- 国民や政府機関、国内民間企業に対して国産の先端技術や学術界の研究成果に基づく**セキュリティサービスを提供**できる。

- 解析エンジン・インテリジェンスプロバイダ（大学や民間企業）に対して、開発した独自のセキュリティ技術をテストする環境と解析対象のデータを提供することで、**研究開発を促進**する。特に国内研究者が実サービス提供に耐える実用的なセキュリティ研究に取り組むことを促す。

- 上記の効果が相乗効果を生み、データ負けの**負のスパイラルからの脱却**により、国内セキュリティ産業、学術研究の育成と独自インテリジェンス蓄積が推進される。

実現に向けた課題

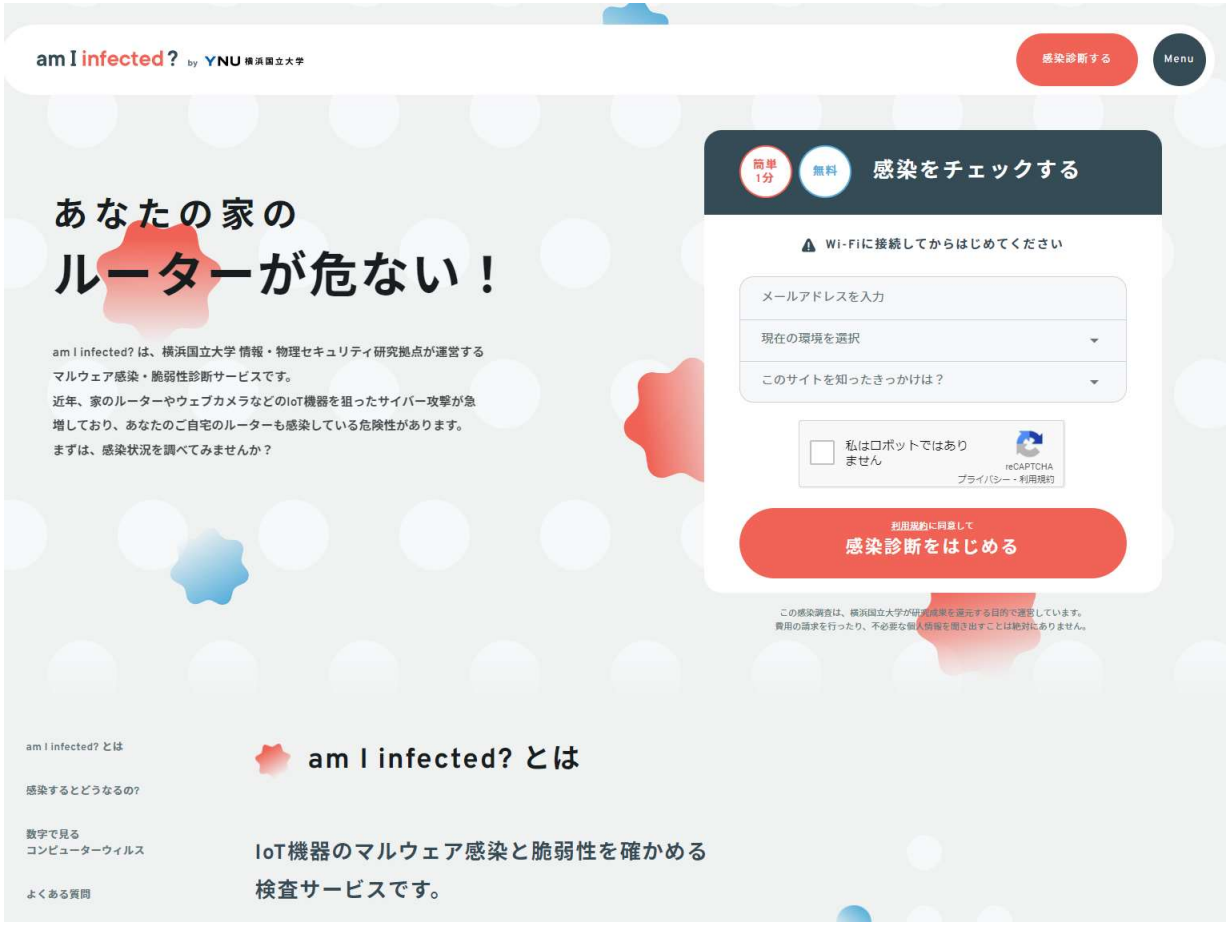
- 統合型セキュリティ（インテリジェンス）検査サービスプラットフォームは現在国内に存在しない。この新規構築、運用には多くのコストが掛かる

- 国産の解析エンジン、インテリジェンスを提供する技術、体力、能力のある研究組織（民間企業、大学）が限られる。何らかの資金面でのサポートが必要（大学研究室は外部資金がなければ人員を確保して大型プロジェクトに参画できない）

- 単一サービスであれば一組織で出来ることもある

スモールスタート　その①

横浜国大発 IoTセキュリティチェックサービス am I infected?



https://amii.ynu.codes/

おわりに

これまで！

- サイバー攻撃そのものの観測、対策を実施

今！

- サイバー攻撃の背景にあるサイバー攻撃ビジネスのエコシステムの観測

これから！

- サイバー攻撃、不正に関連する情報が集まる**エコシステムを作り**、研究開発を活性化したい

横浜国立大学　大学院環境情報研究院/先端科学高等研究院
吉岡克成，yoshioka@ynu.ac.jp
http://yoshioka.ynu.ac.jp

謝辞1：本研究の一部は情報通信研究機構委託研究「Web媒介型攻撃対策技術の実用化に向けた研究開発（H28-R2）」により得られた成果です。
謝辞2：本研究の一部は総務省委託研究「IoT機器に関する脆弱性調査等の実施（H29）」により得られた成果です。
謝辞3：本研究は総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「電波の有効利用のためのIoTマルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含みます。
謝辞4：本研究の一部は総務省「重要IoT機器のセキュリティ対策に係る調査の請負」（NTTコミュニケーションズ株式会社との共同研究として実施（R2）」により得られた成果です。
謝辞5: 本研究の一部は戦略的イノベーション創造プログラム（SIP）第2期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査研究（国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務として実施）により得られた成果です。
謝辞6: 本研究は国立研究開発法人情報通信研究機構の委託研究（05201）によって実施された成果を含みます。